Tesi di Laurea

ARITHMETIC OF
MODULAR FORMS

22 settembre 2017

Candidata
Nirvana Coppola

Relatori
Prof. Massimo Bertolini
Prof. Roberto Dvornicich

Controrelatore
Dr. Davide Lombardo

Anno accademico 2016/2017
## Contents

1 **Tools** .......................... 7
   1.1 Modular Forms ................. 7
   1.2 Hecke Operators .............. 12
      1.2.1 A generalization .......... 21
   1.3 The Petersson inner product .... 22
      1.3.1 The adjoints of Hecke operators ... 24
   1.4 Oldforms and newforms ........ 27
      1.4.1 Eigenforms ............ 31
   1.5 Eisenstein series ............ 33

2 **Deligne-Serre’s Theorem** ...... 37
   2.1 A review of Number Theory .... 37
   2.2 Galois representations ....... 42
   2.3 Deligne-Serre’s Theorem ....... 43
      2.3.1 A result by Rankin ...... 44
      2.3.2 \( \ell \)-adic representations and reduction modulo \( \ell \) ... 48
      2.3.3 A bound on the order of certain subgroups of \( \text{GL}_2(\mathbb{F}_\ell) \) 51
      2.3.4 Proof of Deligne-Serre’s Theorem .... 53

3 **Serre’s Conjecture** .......... 57
   3.1 Artin conductor ............... 57
   3.2 Statement of Serre’s conjecture ... 60
   3.3 Serre’s epsilon-conjecture ... 62
   3.4 Examples ...................... 63
      3.4.1 Case where \( \rho \) has dihedral image ... 64
      3.4.2 Case where \( F = \mathbb{F}_3 \) ... 65
   3.5 Fermat’s Last Theorem ......... 65
Introduction

The main purpose of this work is to present Deligne-Serre’s Theorem and some of its consequences. Suppose given a modular form \( f \) of given level, and of type \((1, \varepsilon)\), where \( \varepsilon \) is a Dirichlet character. Suppose also that \( f \) is an eigenform for certain operators called Hecke operators. Then there exists a Galois representation, namely a representation of the Galois group of an algebraic closure of \( \mathbb{Q} \) over \( \mathbb{Q} \), that takes values in \( \text{GL}_2(\mathbb{C}) \), which is associated to the modular form \( f \), in a sense to be explained in Chapter 2 of this work.

The thesis is structured as follows. In Chapter 1, a series of tools are presented, in order to understand the statement of Deligne-Serre’s Theorem. In particular, we define modular forms of given level and weight, cusp forms, Dirichlet characters, Hecke operators of first and second type, Eisenstein series and particular spaces of cusp forms, namely the space of oldforms and the space of newforms. The latter is particularly important, since it has a basis of Eigenfunction for all but finitely many Hecke operators.

In Chapter 2, we introduce Galois representations, which are linear representations of the absolute Galois group of \( \mathbb{Q} \). More precisely, they are continuous homomorphisms: \( \text{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \text{GL}_d(K) \), where \( K \) is either the complex field \( \mathbb{C} \), a finite field or a \( \ell \)-adic field, each with a suitable topology. Then we state and prove Deligne-Serre’s Theorem, following the paper in [4]. In the proof we will use a result by Rankin, giving a bound to the sum \( \sum |a_p|^2 p^{-s} \), a theorem on \( \ell \)-adic representations that allows us to find a family of representation over finite fields attached to a given modular form, and finally a bound on the order of the subgroups of \( \text{GL}_2(\mathbb{F}_\ell) \) which satisfy a given condition.

In Chapter 3, we explain Serre’s Conjecture, which states a problem that is a converse to Deligne-Serre’s Theorem: given a representation \( \rho \) of the absolute Galois group of \( \mathbb{Q} \), is it possible to find a modular form to which \( \rho \) is attached in the sense of Deligne-Serre’s Theorem? Serre conjectures that, if \( \rho : G \to \text{GL}_2(F) \) is an odd irreducible representation modulo \( p \), then the answer is positive. In particular, he states that it is possible to find a form that is also a newform, and he finds a recipe for the level, weight and character of it. This conjecture has been fully proved by Khare and Wintenberger. In this thesis, first we will explain Serre’s recipe and
some of the most significant results, namely the starting points to prove a weaker conjecture, known as Serre’s epsilon-conjecture, which are Mazur’s and Ribet’s Theorem, and a more recent result, proved by Diamond. Then we will briefly show how Serre’s Conjecture can be proven in two particular cases. Finally, as an interesting application, we will explain Fermat’s Last Theorem and how it is related to Serre’s Conjecture.
Chapter 1

Tools

In this chapter we provide most of the tools that are necessary for the proof of Deligne-Serre’s Theorem and to explain Serre’s Conjectures.

1.1 Modular Forms

Let us consider the group $\text{SL}_2(\mathbb{Z})$, also called modular group, consisting of all 2-by-2 matrices with integer entries and determinant 1:

$$\text{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Z}, \quad ad - bc = 1 \right\}.$$

We can see each element of this group as an automorphism of the Riemann Sphere $\hat{\mathbb{C}} = \mathbb{C} \cup \{\infty\}$ in the following way:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} (z) = \frac{az + b}{cz + d}$$

where $\infty$ maps to $\frac{a}{c}$ and $-\frac{d}{c}$ maps to $\infty$, if $c \neq 0$; otherwise $\infty$ maps to $\infty$.

Let $\mathcal{H}$ be the upper half plane in $\mathbb{C}$, $\mathcal{H} = \{ z \in \mathbb{C} : \Im(z) > 0 \}$. Then it is easy to show that for each $\gamma \in \text{SL}_2(\mathbb{Z})$, $\gamma(\mathcal{H}) \subseteq \mathcal{H}$: if $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ and $z = u + iv \in \mathcal{H}$:

$$\Im(\gamma z) = \Im\left( \frac{az + b}{cz + d} \right) = \Im\left( \frac{au + b +iva}{cu + d + ivc} \right) = \frac{v \det(\gamma)}{(cu + d)^2 + (vc)^2} = \frac{v}{|cz + d|^2}.$$

Thus if $v = \Im(z) > 0$ then also $\Im(\gamma z) > 0$. Moreover, the group $\text{SL}_2(\mathbb{Z})$ acts on $\mathcal{H}$, since $Iz = z$ and $(\gamma \gamma')z = \gamma(\gamma'z)$. The first equality is obvious,
the second holds because:

\[
\frac{a'd'z + b'}{c'd'z + d'} + b = \frac{(aa' + bc')z + ab' + bd'}{(ca' + dc')z + (cb' + dd')}
\]

and

\[
\begin{pmatrix}
a & b \\
c & d
\end{pmatrix}
\begin{pmatrix}
a' & b' \\
c' & d'
\end{pmatrix}
= 
\begin{pmatrix}
aa' + bc' & ab' + bd' \\
ca' + dc' & cb' + dd'
\end{pmatrix}.
\]

Now we are ready to define modular forms.

**Definition 1.1.** Let \( k \) be an integer; a meromorphic function \( f : \mathbb{H} \to \mathbb{C} \) is a weakly modular form of weight \( k \) if

\[
f(\gamma(z)) = (cz + d)^k f(z)
\]

for \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) \) and \( z \in \mathbb{H} \).

Such a function is \( \mathbb{Z} \)-periodic - this is easily seen setting \( \gamma = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \) in the definition above - and so there exists a function \( g : D' \to \mathbb{C} \) such that \( f(z) = g(e^{2\pi iz}) \), where

\[
D' = \{ q \in \mathbb{C} : |q| < 1 \} \setminus \{0\}.
\]

If in addition \( f \) is holomorphic on \( \mathbb{H} \), then \( g \) is holomorphic on \( D' \) by composition, so it has a Laurent expression

\[
g(q) = \sum_{n \in \mathbb{Z}} a_n q^n
\]

for \( q \in D' \). Moreover, \( q \to 0 \) as \( \Im(z) \to \infty \), so it is natural to say that \( f \) is holomorphic at \( \infty \) if \( g \) extends holomorphically to \( q = 0 \). In this case, \( f \) has a Fourier expansion:

\[
f(z) = g(e^{2\pi iz}) = \sum_{n=0}^{\infty} a_n(f)e^{2\pi iz}.
\]

**Definition 1.2.** Let \( k \) be an integer; a function \( f : \mathbb{H} \to \mathbb{C} \) is a modular form of weight \( k \) if it is holomorphic on \( \mathbb{H} \), weakly modular of weight \( k \) and holomorphic at \( \infty \).

A special class of modular forms is given by the **cusp forms**, which are the modular forms whose Fourier expansion has leading coefficient \( a_0(f) = 0 \).
1.1. MODULAR FORMS

The set of modular forms of weight $k$ is denoted $\mathcal{M}_k(\text{SL}_2(\mathbb{Z}))$, the subset of cusp form is $\mathcal{S}_k(\text{SL}_2(\mathbb{Z}))$. In particular, a modular form is a cusp form if

$$\lim_{\Im(z) \to \infty} f(z) = 0.$$

We also call the limit point $\infty$ the cusp of $\text{SL}_2(\mathbb{Z})$ and say that a cusp form vanishes at the cusp.

In general we can replace the modular group $\text{SL}_2(\mathbb{Z})$ with a subgroup $\Gamma$ in the above definitions, thus obtaining the notion of (weakly) modular form with respect to $\Gamma$. Our main concern will be the case where $\Gamma$ is a congruence subgroup.

**Definition 1.3.** Let $N$ be a positive integer; the principal congruence subgroup of level $N$ is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod{N}, \ b \equiv c \equiv 0 \pmod{N} \right\}.$$

A subgroup $\Gamma$ of $\text{SL}_2(\mathbb{Z})$ is a congruence subgroup if there exists $N \in \mathbb{Z}^+$ such that $\Gamma(N) \subseteq \Gamma$; if $N$ is the smallest integer with this property, $\Gamma$ is said to be of level $N$.

The most important congruence subgroups of level $N$ are the following.

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\},$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : a \equiv d \equiv 1 \pmod{N}, \ c \equiv 0 \pmod{N} \right\}.$$

We can also re-define weakly modular forms introducing the factor of automorphy and the weight-$k$ operator of a matrix $\gamma \in \text{SL}_2(\mathbb{Z})$.

**Definition 1.4.** Given $\gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$, the factor of automorphy $j(\gamma, z)$ for $z \in \mathcal{H}$ is

$$j(\gamma, z) = cz + d;$$

for an integer $k$, the weight-$k$ operator $[\gamma]_k$ on functions $f : \mathcal{H} \to \mathbb{C}$ is given by

$$(f[\gamma]_k)(z) = j(\gamma, z)^{-k} f(\gamma z)$$

for $z \in \mathcal{H}$. 
Hence we can say that a meromorphic function \( f : \mathcal{H} \to \mathbb{C} \) is weakly modular of weight \( k \) with respect to \( \Gamma \) if it satisfies the relation

\[
f[\gamma]_k = f
\]

for every \( \gamma \in \Gamma \). Some basic properties of these operators are stated in the following lemma.

**Lemma 1.5.** For all \( \gamma, \gamma' \in \text{SL}_2(\mathbb{Z}) \) and \( z \in \mathcal{H} \),

(a) \( j(\gamma \gamma', z) = j(\gamma, \gamma' z) j(\gamma', z) \);

(b) \( (\gamma \gamma') z = \gamma(\gamma' z) \);

(c) \( [\gamma \gamma']_k = [\gamma]_k [\gamma']_k \);

(d) \( \Im(\gamma z) = \frac{\Im(z)}{|j(\gamma, z)|^2} \);

(e) \( \frac{d(\gamma z)}{dz} = \frac{1}{j(\gamma, z)^2} \).

**Proof.** Properties (a) – (d) easily follow from what proven above. For (e) we can write

\[
\gamma z' - \gamma z = \frac{\det(\gamma)(z' - z)}{j(\gamma, z) j(\gamma, z')}
\]

thus \( \frac{\gamma z' - \gamma z}{z' - z} = \frac{1}{j(\gamma, z) j(\gamma, z')} \) and so

\[
\frac{d(\gamma z)}{dz} = \lim_{z' \to z} \frac{\gamma z' - \gamma z}{z' - z} = \frac{1}{j(\gamma, z)^2},
\]

and this gives (e). \( \square \)

In order to define modular forms with respect to a congruence subgroup \( \Gamma \), consider \( h \) minimal such that \( \Gamma \) contains the matrix \( \begin{pmatrix} 1 & h \\ 0 & 1 \end{pmatrix} \); such \( h \) always exists and divides \( N \) if \( \Gamma \) is of level \( N \). Thus every function \( f : \mathcal{H} \to \mathbb{C} \) which is weakly modular of weight \( k \) with respect to \( \Gamma \) is \( h \)-periodic and there exists \( g : D' \to \mathbb{C} \) such that

\[
f(z) = g(e^{2\pi iz/h});
\]

if such a function \( f \) is holomorphic, then also \( g \) is holomorphic and has a Laurent expansion

\[
g(q_h) = \sum_n a_n q_h^n,
\]
1.1. MODULAR FORMS

where \( q_h = e^{2\pi i z/h}; \) if \( g \) extends holomorphically at \( q_h = 0, \) \( f \) is said to be holomorphic at \( \infty, \) so it has a Fourier expansion

\[
f(z) = g(e^{2\pi i z/h}) = \sum_{n=0}^{\infty} a_n e^{2\pi i z/h}.
\]

The limit points, or cusps, of a congruence subgroup \( \Gamma \) are not only \( \infty, \) but also all the rational points in \( \mathbb{Q} \subseteq \mathbb{C}, \) identified under \( \Gamma \)-equivalence, i.e. \( r, s \in \mathbb{Q} \) are equivalent if and only if there is \( \gamma \in \Gamma \) such that \( \gamma r = s. \) For example, the only cusp of \( SL_2(\mathbb{Z}) \) is \( \infty. \) We now need to clarify what is the meaning of holomorphic at a cusp; writing any \( s \in \mathbb{Q} \) as \( s = \alpha(\infty), \) where \( \alpha \in SL_2(\mathbb{Z}), \) we have that \( f[\alpha]_k \) is weakly modular of weight \( k \) with respect to \( \alpha^{-1}\Gamma\alpha, \) holomorphic on \( \mathcal{H}, \) and we can check whether it is holomorphic at \( \infty; \) in this case, we say that \( f \) is holomorphic at the cusp \( s. \) Now we are ready to give the final definition of a modular form.

**Definition 1.6.** Let \( \Gamma \) be a congruence subgroup of \( SL_2(\mathbb{Z}) \) and let \( k \) be an integer. A function \( f : \mathcal{H} \to \mathbb{C} \) is a modular form of weight \( k \) with respect to \( \Gamma \) if:

- \( f \) is holomorphic;
- \( f \) is weakly modular of weight \( k \) with respect to \( \Gamma; \)
- \( f[\alpha]_k \) is holomorphic at \( \infty \) for all \( \alpha \in SL_2(\mathbb{Z}). \)

It is called a cusp form of weight \( k \) with respect to \( \Gamma \) if in addition \( a_0 = 0 \) in the Fourier expansion of \( f[\alpha]_k \) for all \( \alpha \in SL_2(\mathbb{Z}). \)

The set of modular forms of weight \( k \) with respect to \( \Gamma \) is denoted \( \mathcal{M}_k(\Gamma), \) the subset of the cusp forms is \( \mathcal{S}_k(\Gamma). \)

The modular forms involved in Deligne-Serre’s Theorem are the ones of type \((k, \varepsilon)\) with respect to \( \Gamma_0(N), \) which are a particular class of modular forms of weight \( k \) with respect to \( \Gamma_1(N). \) Here, \( \varepsilon \) is a Dirichlet character mod \( N, \) as defined below.

**Definition 1.7.** A Dirichlet character mod \( N \) is a homomorphism

\[
\varepsilon : \left( \frac{\mathbb{Z}}{N\mathbb{Z}} \right)^* \to \mathbb{C}^*.
\]

It is called even if \( \varepsilon(-1) = 1, \) odd if \( \varepsilon(-1) = -1. \)

Let \( k \) be an integer and \( \varepsilon \) a Dirichlet character of the same parity, that is to say \( \varepsilon(-1) = (-1)^k. \) We know that a modular form of weight \( k \) with respect to \( \Gamma_1(N) \) satisfies the relation

\[
f \left( \frac{az + b}{cz + d} \right) = (cz + d)^k f(z)
\]
for \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \gamma \in \Gamma_1(N) \). Now, if \( f \) is such a function and \( \gamma \in \Gamma_0(N) \), the form \( f[\gamma]_k \) only depends on \( d \) as an element of \( \left( \frac{\mathbb{Z}}{N\mathbb{Z}} \right)^* \). In particular, if this dependence is given by a Dirichlet character \( \varepsilon \), we get modular forms of type \((k, \varepsilon)\).

**Definition 1.8.** A modular form of weight \( k \) with respect to \( \Gamma_1(N) \) is called of type \((k, \varepsilon)\) with respect to \( \Gamma_0(N) \) if for each \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N) \):

\[
f\left( \begin{pmatrix} az + b \\ cz + d \end{pmatrix} \right) = \varepsilon(d)(cz + d)^k f(z).
\]

### 1.2 Hecke Operators

We now define the double coset operator; the Hecke operators will be particular cases of it. Let \( \Gamma_1 \) and \( \Gamma_2 \) be congruence subgroups of \( \text{SL}_2(\mathbb{Z}) \). We can also view them as subgroups of \( \text{GL}_2^+ (\mathbb{Q}) \), that is the subgroup of \( \text{GL}_2(\mathbb{Q}) \) consisting of the matrices whose determinant is positive.

**Definition 1.9.** For each \( \alpha \in \text{GL}_2^+ (\mathbb{Q}) \), the set

\[
\Gamma_1 \alpha \Gamma_2 = \{ \gamma_1 \alpha \gamma_2 : \gamma_i \in \Gamma_i \}
\]

is a double coset in \( \text{GL}_2^+ (\mathbb{Q}) \).

The group \( \Gamma_1 \) acts on \( \Gamma_1 \alpha \Gamma_2 \) by left multiplication; an orbit of this action takes the form \( \Gamma_1 \beta \), where \( \beta = \gamma_1 \alpha \gamma_2 \) is a representative of the orbit; the orbit space \( \Gamma_1 \alpha \Gamma_2 / \Gamma_1 \) is the disjoint union of the orbits, \( \bigcup_i \Gamma_1 \beta_i \), for a suitable choice of representatives \( \beta_i \). As a generalization of weight-\( k \) operators, given \( \beta \in \text{GL}_2^+ (\mathbb{Q}) \), we can define the weight-\( k \) \( \beta \) operator \( [\beta]_k \) such that

\[
(f[\beta]_k)(z) = (\det \beta)^{k-1} j(\beta, z)^{-k} f(\beta z),
\]

with the same notations as in the previous section.

**Definition 1.10.** For congruence subgroups \( \Gamma_1 \) and \( \Gamma_2 \) of \( \text{SL}_2(\mathbb{Z}) \) and \( \alpha \in \text{GL}_2^+ (\mathbb{Q}) \), the weight-\( k \) \( \Gamma_1 \alpha \Gamma_2 \) operator takes functions \( f \in \mathcal{M}_k(\Gamma_1) \) to

\[
f[\Gamma_1 \alpha \Gamma_2]_k = \sum_i f[\beta_i]_k,
\]

where \( \Gamma_1 \alpha \Gamma_2 = \bigcup_i \Gamma_1 \beta_i \) is a disjoint union.

First of all, we have to show that the sum is finite. In order to do so, we will prove the following lemmas.
Lemma 1.11. Let $\Gamma$ be a congruence subgroup of $\text{SL}_2(\mathbb{Z})$ and let $\alpha \in \text{GL}_2^+(\mathbb{Q})$. Then $\alpha^{-1}\Gamma\alpha \cap \text{SL}_2(\mathbb{Z})$ is another congruence subgroup.

Proof. Let $\tilde{N}$ be an integer such that $\Gamma(\tilde{N}) \subseteq \Gamma$ and the matrices $\tilde{N}\alpha$ and $\tilde{N}\alpha^{-1}$ have integer entries. Set $N = \tilde{N}^3$; then $\alpha\Gamma(N)\alpha^{-1} \subseteq \Gamma$, indeed:

$$
\alpha\Gamma(N)\alpha^{-1} \subseteq \alpha(I + NM_2(\mathbb{Z}))\alpha^{-1} = I + \tilde{N}(\tilde{N}\alpha)M_2(\mathbb{Z})(\tilde{N}\alpha^{-1}) \subseteq I + \tilde{N}M_2(\mathbb{Z}),
$$

thus $\alpha\Gamma(N)\alpha^{-1} \subseteq \text{SL}_2(\mathbb{Z}) \cap I + \tilde{N}M_2(\mathbb{Z}) = \Gamma(\tilde{N})$.

This proves that $\Gamma(N) \subseteq \alpha^{-1}\Gamma\alpha \cap \text{SL}_2(\mathbb{Z})$, so the latter is a congruence subgroup of $\text{SL}_2(\mathbb{Z})$. \hfill $\blacksquare$

Lemma 1.12. Let $\Gamma_1$ and $\Gamma_2$ be two congruence subgroups of $\text{SL}_2(\mathbb{Z})$ and let $\alpha$ in $\text{GL}_2^+(\mathbb{Q})$. Set $\Gamma_3 = \alpha^{-1}\Gamma_1\alpha \cap \Gamma_2$; then left multiplication by $\alpha$:

$$
\Gamma_2 \rightarrow \Gamma_1 \alpha \Gamma_2
$$

induces a natural bijection from $\frac{\Gamma_2}{\Gamma_3}$ to $\frac{\Gamma_1 \alpha \Gamma_2}{\Gamma_1}$.

Proof. The left multiplication by $\alpha$:

$$
\Gamma_2 \rightarrow \Gamma_1 \alpha \Gamma_2
$$

$\gamma_2 \mapsto \alpha \gamma_2$

induces a surjective map

$$
\Gamma_2 \rightarrow \frac{\Gamma_1 \alpha \Gamma_2}{\Gamma_1}
$$

$\gamma_2 \mapsto \Gamma_1 \alpha \gamma_2$.

To prove injectivity of the induced map from $\frac{\Gamma_2}{\Gamma_3}$ to $\frac{\Gamma_1 \alpha \Gamma_2}{\Gamma_1}$, we can see that $\Gamma_1 \alpha \gamma_2 = \Gamma_1 \alpha \gamma'_2$ if and only if $\gamma'_2 \gamma_2^{-1} \in \alpha^{-1}\Gamma_1\alpha$; moreover $\gamma'_2 \gamma_2^{-1} \in \Gamma_2$, and so the condition holds if and only if $\gamma'_2 \gamma_2^{-1} \in \Gamma_3$. The lemma follows. \hfill $\blacksquare$

Lemma 1.13. Any two congruence subgroups $\Gamma_1$ and $\Gamma_2$ are commensurable, meaning that

$$
[\Gamma_1 : \Gamma_1 \cap \Gamma_2] \text{ and } [\Gamma_2 : \Gamma_1 \cap \Gamma_2]
$$

are finite.

Proof. Let $N_1$, $N_2$ be natural numbers such that $\Gamma(N_i) \subseteq \Gamma_i$ and let $N_3 = \text{lcm}(N_1, N_2)$. 


We can notice that for each $N \in \mathbb{Z}^+$, the homomorphism
\[
\text{SL}_2(\mathbb{Z}) \to \text{SL}_2\left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)
\]
\[
\begin{pmatrix} a & b \\ c & d \end{pmatrix} \mapsto \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix}
\]
is surjective with kernel $\Gamma(N)$; hence $|\text{SL}_2(\mathbb{Z}) : \Gamma(N)| = |\text{SL}_2\left(\frac{\mathbb{Z}}{N\mathbb{Z}}\right)|$ is finite. In particular, for each congruence subgroup of $\text{SL}_2(\mathbb{Z})$ of level $N$, the index $[\Gamma : \Gamma(N)]$ is finite.

Now $\Gamma(N_3) \subseteq \Gamma_1 \cap \Gamma_2$ and, since $[\Gamma_1 : \Gamma(N_3)]$ and $[\Gamma_2 : \Gamma(N_3)]$ are finite, also $[\Gamma_1 : \Gamma_1 \cap \Gamma_2]$ and $[\Gamma_2 : \Gamma_1 \cap \Gamma_2]$ are.

In particular, since $\alpha^{-1}\Gamma_1 \cap \text{SL}_2(\mathbb{Z})$ is a congruence subgroup of $\text{SL}_2(\mathbb{Z})$ by Lemma 1.11, the space $\frac{\Gamma_2}{\Gamma_3}$ is finite and so is $\frac{\Gamma_1\alpha\Gamma_2}{\Gamma_1}$, by Lemma 1.12. Hence in Definition 1.10 the sum is taken over a finite set of representatives $\{\beta_i\}_i$.

Now we can prove that the weight-$k$ $\Gamma_1 \alpha \Gamma_2$ operator is well defined.

**Lemma 1.14.** If $\beta$ and $\beta'$ are two representatives for the same orbit of $\Gamma_1 \alpha \Gamma_2$, then
\[
f[\beta]_k = f[\beta']_k
\]
for every $f \in M_k(\Gamma_1)$.

**Proof.** If $\Gamma_1 \beta = \Gamma_1 \beta'$, then writing $\beta = \gamma_1 \alpha \gamma_2$ and $\beta' = \gamma'_1 \alpha \gamma'_2$ we have that $\alpha \gamma_2 \in \Gamma_1 \alpha \gamma'_2$, hence
\[
\delta = (\alpha \gamma_2)(\alpha \gamma'_2)^{-1} \in \Gamma_1.
\]
If $f \in M_k(\Gamma_1)$, then $f[\gamma \phi]_k = f[\phi]_k$ for all $\gamma \in \Gamma_1$ and $\phi \in \text{GL}_2^+(\mathbb{Q})$. Thus if $f \in M_k(\Gamma_1)$, then $f[\delta(\alpha \gamma'_2)]_k = f[\alpha \gamma'_2]_k$, which means $f[\alpha \gamma_2]_k = f[\alpha \gamma'_2]_k$. Moreover
\[
f[\beta]_k = f[\gamma_1 \alpha \gamma_2]_k = f[\alpha \gamma_2]_k = f[\alpha \gamma'_2]_k = f[\beta']_k,
\]
and the lemma follows.

Next we show that the weight-$k$ $\Gamma_1 \alpha \Gamma_2$ operator takes modular forms with respect to $\Gamma_1$ to modular forms with respect to $\Gamma_2$ and cusp forms to cusp forms.

**Lemma 1.15.** For each $f \in M_k(\Gamma_1)$ the transformed $f[\Gamma_1 \alpha \Gamma_2]_k$ is $\Gamma_2$-invariant.
1.2. HECKE OPERATORS

Proof. First we notice that each \( \gamma_2 \in \Gamma_2 \) permutes the orbits of \( \frac{\Gamma_1 \alpha \Gamma_2}{\Gamma_1} \) acting by right multiplication, thus if \( \{ \beta_i \} \) is a set of representatives, so is \( \{ \beta_i \gamma_2 \} \). Hence

\[
(f[\Gamma_1 \alpha \Gamma_2]|_{k})[\gamma_2]_k = \sum_i f[\beta_i \gamma_2]_k = f[\Gamma_1 \alpha \Gamma_2]_k,
\]

so \( f[\Gamma_1 \alpha \Gamma_2]_k \) is weight-\( k \) invariant under \( \Gamma_2 \).

Lemma 1.16. For each \( f \in \mathcal{M}_k(\Gamma_1) \) the transformed \( f[\Gamma_1 \alpha \Gamma_2]_k \) is holomorphic at the cusps.

Proof. We can note that if \( f \in \mathcal{M}_k(\Gamma_1) \), then for each \( \gamma \in \text{GL}_2^+(\mathbb{Q}) \), the function \( g = f[\gamma]_k \) is holomorphic at \( \infty \). Moreover the sum of a finite number of functions that are holomorphic at \( \infty \) is holomorphic at \( \infty \). Now, if \( \delta \in \text{SL}_2(\mathbb{Z}) \), then \( (f[\Gamma_1 \alpha \Gamma_2]|_{k})[\delta]_k \) is a sum of functions of the form \( g_i = f[\beta_i \delta]_k \), which are holomorphic at \( \infty \) by what just remarked.

Finally, if \( f \in \mathcal{S}_k(\Gamma_1) \), the function \( f[\gamma]_k \) vanishes at \( \infty \) for every \( \gamma \in \text{GL}_2^+(\mathbb{Q}) \). Proceeding as in the proof of Lemma 1.16 we can show that \( f[\Gamma_1 \alpha \Gamma_2]_k \in \mathcal{S}_k(\Gamma_2) \).

We now introduce two operators on \( \mathcal{M}_k(\Gamma_1(N)) \), where \( N \) is a positive integer. The map \( \Gamma_0(N) \to (\mathbb{Z}/N\mathbb{Z})^* \) taking \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) to \( d \) is a surjective homomorphism, with kernel \( \Gamma_1(N) \), thus it induces a isomorphism

\[
\frac{\Gamma_0(N)}{\Gamma_1(N)} \to (\mathbb{Z}/N\mathbb{Z})^*.
\]

and \( \Gamma_1(N) \) is a normal subgroup of \( \Gamma_0(N) \). If we take \( \Gamma_1 = \Gamma_2 = \Gamma_1(N) \) and \( \alpha \in \Gamma_0(N) \), the double coset operator \( [\Gamma_1 \alpha \Gamma_2]_k \) acts as \( [\alpha]_k \), defining an isomorphism of \( \mathcal{M}_k(\Gamma_1(N)) \). Indeed \( \Gamma_1 \alpha \Gamma_1 = \Gamma_1 \alpha \Gamma_1^{-1} \Gamma_1 \alpha = \Gamma_1 \alpha \), so the only representative for the orbits of \( \Gamma_1 \alpha \) is \( \alpha \) itself. Thus the group \( \Gamma_0(N) \) acts on \( \mathcal{M}_k(\Gamma_1(N)) \) and the restriction of the action to \( \Gamma_1(N) \) is trivial, thus defining an action of the quotient \( (\mathbb{Z}/N\mathbb{Z})^* \) on \( \mathcal{M}_k(\Gamma_1(N)) \).

Definition 1.17. For each \( d \in \mathbb{Z} \) such that \( (d,N) = 1 \), we define a diamond operator (or Hecke operator of the first kind) \( \langle d \rangle \) as follows. Let \( \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N) \) be a matrix such that \( \delta \equiv d \pmod{N} \); then \( \langle d \rangle \) is given by

\[
\langle d \rangle : \mathcal{M}_k(\Gamma_1(N)) \to \mathcal{M}_k(\Gamma_1(N))
\]

\[
f \mapsto f[\alpha]_k \text{ for } \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N), \ \delta \equiv d \pmod{N}.
\]
CHAPTER 1. TOOLS

Notice that by construction \( \langle d \rangle \) depends only on \( d \) modulo \( N \), in particular it is independent on the choice of \( \alpha \).

Another particular case of weight-\( k \) double coset operator is defined when \( \Gamma_1 = \Gamma_2 = \Gamma_1(N) \) as above, and \( \alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \) and \( p \) is prime. Hence we have the following definition.

**Definition 1.18.** Let \( p \) be a prime number. The operator \( T_p \), or second type of Hecke operator is given by:

\[
T_p : M_k(\Gamma_1(N)) \to M_k(\Gamma_1(N))
\]

\[
f \mapsto f \left[ \Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N) \right]_k.
\]

It is easy to see that the double coset here is given by

\[
\left\{ \gamma \in M_2(\mathbb{Z}) : \gamma \equiv \begin{pmatrix} 1 & * \\ 0 & p \end{pmatrix} \pmod{N}, \det \gamma = p \right\}.
\]

We will need some properties of these two kinds of Hecke operators.

**Lemma 1.19.** The operators \( \langle d \rangle \) and \( T_p \) for \( d \in \mathbb{Z} \) and \( p \) prime commute.

**Proof.** Let \( \alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \). First we can see that for \( \gamma \in \Gamma_0(N) \), it holds:

\[
\gamma \alpha \gamma^{-1} \equiv \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} d & -b \\ 0 & a \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & p \end{pmatrix} \pmod{N},
\]

and so the double cosets \( \Gamma_1(N) \alpha \Gamma_1(N) \) and \( \Gamma_1(N) \gamma \alpha \gamma^{-1} \Gamma_1(N) \) are equal. So, considering also that \( \Gamma_1(N) \) is normal in \( \Gamma_0(N) \):

\[
\Gamma_1(N) \alpha \Gamma_1(N) = \Gamma_1(N) \gamma \alpha \gamma^{-1} \Gamma_1(N) = \gamma \Gamma_1(N) \alpha \Gamma_1(N) \gamma^{-1} =
\]

\[
= \gamma \bigcup_i \Gamma_1(N) \beta_i \gamma^{-1} = \bigcup_i \Gamma_1(N) \gamma \beta_i \gamma^{-1},
\]

where \( \Gamma_1(N) \alpha \Gamma_1(N) = \bigcup_i \Gamma_1(N) \beta_i \). Hence \( \bigcup_i \Gamma_1(N) \beta_i \gamma = \bigcup_i \Gamma_1(N) \gamma \beta_i \). Thus for each \( f \in M_k(\Gamma_1(N)) \) and \( \gamma \in \Gamma_0(N) \) such that the lower right entry is \( \delta \equiv d \pmod{N} \),

\[
\sum_i f[\beta_i \gamma]_k = \sum_i f[\gamma \beta_i]_k,
\]

so \( \langle d \rangle T_p(f) = T_p \langle d \rangle (f) \).

To find an explicit representation of \( T_p \) we now prove the following proposition.
Proposition 1.20. Let $N \in \mathbb{Z}^+$, let $\Gamma_1 = \Gamma_2 = \Gamma_1(N)$ and let $\alpha = \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix}$ where $p$ is prime. The operator $T_p = [\Gamma_1 \alpha \Gamma_2]_k$ on $\mathcal{M}_k(\Gamma_1(N))$ is given by

$$T_p(f) = \begin{cases} \sum_{i=0}^{p-1} f \left( \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} \right)_k & p \mid N, \\ \sum_{i=0}^{p-1} f \left( \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} \right)_k + f \left[ \begin{pmatrix} m & n \\ N & p \end{pmatrix} \left( \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right) \right]_k & p \nmid N, \end{cases}$$

and in the latter formula it holds $mp - nN = 1$.

Proof. To prove the proposition it suffices to show that a set of representatives for $\frac{\Gamma_1 \alpha \Gamma_2}{\Gamma_1}$ is:

$$\left\{ \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} : 0 \leq i < p \right\} \quad p \mid N,$$

$$\left\{ \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} : 0 \leq i < p \right\} \cup \left\{ \begin{pmatrix} m & n \\ N & p \end{pmatrix} \left( \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right) \right\} \quad p \nmid N.$$

We know from Lemma 1.12 that a set of representatives for $\frac{\Gamma_1 \alpha \Gamma_2}{\Gamma_2}$ corresponds to one for $\frac{\Gamma_2}{\Gamma_3}$ via the left multiplication by $\alpha$. In our case, $\Gamma_2 = \Gamma_1(N)$ and $\Gamma_3 = \Gamma_1(N) \cap \alpha^{-1} \Gamma_1(N) \alpha$.

Let $\Gamma^0(p)$ and $\Gamma^0_1(N,p)$ be as follows.

$$\Gamma^0(p) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & 0 \\ * & * \end{pmatrix} \pmod{p} \right\},$$

$$\Gamma^0_1(N,p) = \Gamma_1(N) \cap \Gamma^0(p).$$

Then it is easy to see that $\Gamma_3 = \Gamma^0_1(N,p)$.

- If $\gamma \in \Gamma_3$, then it takes the form

$$\begin{pmatrix} 1 & 0 \\ 0 & p^{-1} \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \in \Gamma_1(N),$$

where $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N)$. So the top right entry of $\gamma$ satisfies $bp \equiv 0 \pmod{p}$, hence $\gamma \in \Gamma^0_1(N,p)$.  


- Vice versa, if \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1^0(N, p) \), then it clearly belongs to \( \Gamma_1(N) \).

We only need to show that \( \alpha \begin{pmatrix} a & b \\ c & d \end{pmatrix} \alpha^{-1} \in \Gamma_1(N) \). We have

\[
\begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & p^{-1} \end{pmatrix} = \begin{pmatrix} a & bp^{-1} \\ pc & d \end{pmatrix},
\]

and if \( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \), then so does \( \begin{pmatrix} a & bp^{-1} \\ pc & d \end{pmatrix} \).

Thus \( \Gamma_3 = \Gamma_1(N) \cap \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z}) : b \equiv 0 \pmod{p} \right\} \). Let us consider the set

\[
\left\{ \gamma_i = \begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix} : 0 \leq i < p \right\}.
\]

Clearly the orbits \( \Gamma_3 \gamma_i \) are all disjoint: if \( \gamma \gamma_i \in \Gamma_3 \gamma_i, \gamma' \gamma_j \in \Gamma_3 \gamma_j \) and \( \gamma \gamma_i = \gamma' \gamma_j \), then \( \gamma_j \gamma_i^{-1} \) should belong to \( \Gamma_3 \), but it does not if \( j \neq i \), because \( j - i \neq 0 \pmod{p} \).

Now let \( \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_1(N) \). Then \( \gamma \in \Gamma_3 \gamma_i \) if and only if \( \gamma \gamma_i^{-1} \in \Gamma_3 \), that happens if and only if the top right entry of \( \gamma \gamma_i^{-1} \) is a multiple of \( p \). We can see that

\[
\gamma \gamma_i^{-1} = \begin{pmatrix} a & b - ia \\ c & d - ic \end{pmatrix},
\]

so the condition we need is \( b - ia \equiv 0 \pmod{p} \). If \( p \nmid a \), then \( i \equiv ba^{-1} \pmod{p} \) satisfies it. Otherwise, there is no such \( i \): if there were, then \( p \mid b \) as well and so \( p \mid \det \gamma = 1 \), which is impossible. Using the fact that \( a \equiv 1 \pmod{N} \), we can show that \( p \mid a \) if and only if \( p \nmid N \). In this case, let

\[
\gamma_\infty = \begin{pmatrix} mp & n \\ N & 1 \end{pmatrix},
\]

where \( mp - Nn = 1 \). Then if \( p \mid a \), \( \gamma \gamma_\infty^{-1} \in \Gamma_3 \), since its top right entry is \( bmp - an \), a multiple of \( p \).

To sum up, a set of representatives for \( \frac{\Gamma_1(N)}{\Gamma_3} \) is

\[
\left\{ \gamma_0, \ldots, \gamma_{p-1} : p \mid N, \gamma_0, \ldots, \gamma_{p-1}, \gamma_\infty : p \nmid N. \right\}
\]
Using the correspondence between $\frac{\Gamma_1(N)\alpha\Gamma_1(N)}{\Gamma_1(N)}$ and $\frac{\Gamma_1(N)}{\Gamma_1(N)}$, recalled above, we find the corresponding representatives for $\frac{\Gamma_1(N)\alpha\Gamma_1(N)}{\Gamma_1(N)}$, which are

$$\beta_i = \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} \text{ for } 0 \leq i < p,$$

$$\beta_\infty = \begin{pmatrix} m & n \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}$$

as we wanted. 

Using Proposition 1.20, we can describe the Fourier coefficients of $T_p(f)$, where $f \in M_k(\Gamma_1(N))$. First we can notice that $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in \Gamma_1(N)$, so $f$ has period 1 and a Fourier expansion

$$f(z) = \sum_{n=0}^{\infty} a_n(f) q^n, \quad q = e^{2\pi i z}.$$

**Proposition 1.21.** Let $f \in M_k(\Gamma_1(N))$ with Fourier expansion as above. Let $1_N$ be the trivial Dirichlet character modulo $N$, such that $1_N(p) = 0$ if $p \mid N$, $1_N(p) = 1$ if $p \nmid N$; then $T_p(f)$ has Fourier coefficients:

$$a_n(T_p f) = a_{np}(f) + 1_N(p)p^{k-1}a_{n/p}(\langle p \rangle f),$$

where $a_{n/p} = 0$ if $p \nmid n$.

**Proof.** Let us first suppose that $p \mid N$. Then $T_p(f) = \sum_{j=0}^{p-1} f \left( \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \right)_k$. We know that

$$f \left( \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \right)_k(z) = p^{k-1}p^{-k} f \left( \frac{z+j}{p} \right) = \frac{1}{p} \sum_{n=0}^{\infty} a_n(f) q^n p_j^\mu p_j^\mu,$$

where $q_p = e^{2\pi i / p}$ and $\mu_p = e^{2\pi i / p}$. Since $\sum_{j=0}^{p-1} \mu_p^{nj} = \begin{cases} 0 & p \mid n \\ p & p \nmid n \end{cases}$, then

$$\sum_{j=0}^{p-1} f \left( \begin{pmatrix} 1 & j \\ 0 & p \end{pmatrix} \right)_k(z) = \frac{1}{p} \sum_{n=0}^{\infty} a_n(f) q_p^n \sum_{j=0}^{p-1} \mu_p^{nj} = \frac{1}{p} \sum_{n\equiv 0 \pmod{(p)}} a_n(f) q_p^n p = \sum_{n=0}^{\infty} a_{np}(f) q^n.$$

Hence if $p \mid N$ then the proposition follows; if $p \nmid N$, there is another term:

$$f \left( \begin{pmatrix} m & n \\ N & p \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right)_k(z) = (\langle p \rangle f) \left( \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right)_k(z) = p^{k-1}(\langle p \rangle f)(pz) = p^{k-1} \sum_{n=0}^{\infty} a_n(\langle p \rangle f) q^{nm},$$

and that concludes the proof.
We can see that if \( \varepsilon \) is another Dirichlet character modulo \( N \) and if \( M_k(N, \varepsilon) \) is the \( \varepsilon \)-eigenspace of the diamond operator:

\[
M_k(N, \varepsilon) = \left\{ f \in M_k(\Gamma_1(N)) : \langle d \rangle f = \varepsilon(d) f \quad \forall d \in \left( \frac{\mathbb{Z}}{N\mathbb{Z}} \right)^* \right\},
\]

then if \( f \in M_k(N, \varepsilon) \) also \( T_p(f) \in M_k(N, \varepsilon) \) and

\[
a_n(T_p f) = a_{np}(f) + \varepsilon(p)p^{k-1}a_{n/p}(f).
\]

Notice that it holds \( M_k(\Gamma_1(N)) = \bigoplus \varepsilon M_k(N, \varepsilon) \) (see [6], §4 and 5 for the proof).

Since the operators \( T_p \) and \( \langle d \rangle \) commute, \( T_p(f) \) is a \( \varepsilon \)-eigenfunction and applying the result of Proposition 1.21 to \( \langle d \rangle f \) the formula follows.

Finally, we will show some other commutation properties of the Hecke operators.

**Proposition 1.22.** Let \( d \) and \( e \) be elements of \( \left( \frac{\mathbb{Z}}{N\mathbb{Z}} \right)^* \) and \( p \) and \( q \) two prime numbers. Then

- \( \langle d \rangle T_p = T_p \langle d \rangle \);
- \( \langle d \rangle \langle e \rangle = \langle e \rangle \langle d \rangle = \langle de \rangle \);
- \( T_p T_q = T_q T_p \).

**Proof.** We have already proven the first property; since both the Hecke operators map \( M_k(N, \varepsilon) \) to itself and since \( M_k(\Gamma_1(N)) = \bigoplus \varepsilon M_k(N, \varepsilon) \) we only need to check the other two properties on arbitrary \( f \in M_k(N, \varepsilon) \).

Since for each \( d \in \left( \frac{\mathbb{Z}}{N\mathbb{Z}} \right)^* \), \( \langle d \rangle f = \varepsilon(d) f \), then

\[
\langle d \rangle \langle e \rangle (f) = \varepsilon(d) \varepsilon(e) f = \varepsilon(\varepsilon e) f,
\]

which is symmetric in \( d \) and \( e \).

As for the last equality, by the previous formula we have:

\[
a_n(T_p(T_q f)) = a_{np}(T_q f) + \varepsilon(p)p^{k-1}a_{n/p}(T_q f) =
\]

\[
=a_{npq}(f) + \varepsilon(q)q^{k-1}a_{np/q}(f) + \varepsilon(p)p^{k-1}(a_{nq/p}(f) + \varepsilon(q)q^{k-1}a_{n/q}(f)) =
\]

\[
=a_{npq}(f) + \varepsilon(q)q^{k-1}a_{np/q}(f) + \varepsilon(p)p^{k-1}a_{nq/p}(f) + \varepsilon(p)\varepsilon(q)q^{k-1}a_{n/q}(f),
\]

that is again symmetric in \( p \) and \( q \). \( \square \)
1.2. HECKE OPERATORS

1.2.1 A generalization

It is possible to extend the definition of Hecke operators to $\langle n \rangle$ and $T_n$ for all $n \in \mathbb{Z}^+$. We know how to define the diamond operator $\langle d \rangle$ for $d \in \mathbb{Z}/N\mathbb{Z}$. Let $n \in \mathbb{Z}^+$ with $(n,N) = 1$; then $\langle n \rangle = \langle \bar{n} \rangle$ where $\bar{n}$ is the class of $n$ modulo $N$ and the latter is the usual diamond operator. If $(n,N) \neq 1$, we just set $\langle n \rangle = 0$. Hence the mapping $n \mapsto \langle n \rangle$ satisfies:

$$\langle nm \rangle = \langle n \rangle \langle m \rangle = \langle m \rangle \langle n \rangle.$$

For the Hecke operator of second type, we need to proceed inductively. Set $T_1 = 1$, that is the identity operator; then, we already know how to define $T_p$ for a prime number $p$. For $n = p^r$, we set

$$T_{p^r} = T_p T_{p^{r-1}} - p^{k-1}(p) T_{p^{r-2}}.$$

As in Proposition 1.22, we can show that $T_{p^r}$ and $T_{q^s}$ commute for all prime numbers $p$ and $q$ and positive integers $r$ and $s$. Finally, we extend the definition to $n$ setting

$$T_n = \prod T_{p_i^{e_i}} \text{ where } n = \prod p_i^{e_i}.$$

Again $T_n$ and $T_m$ commute if $(n,m) = 1$. With the same techniques as in Proposition 1.21, we can compute the Fourier expansion of $T_n(f)$, where $f \in \mathcal{M}_k(\Gamma_1(N))$. The coefficients are given in the following Proposition.

**Proposition 1.23.** Let $f \in \mathcal{M}_k(\Gamma_1(N))$ have Fourier expansion

$$f(z) = \sum_{m=0}^{\infty} a_m(f) q^m$$

where $q = e^{2\pi i z}$. Then for all $n \in \mathbb{Z}^+$, $T_n(f)$ has Fourier expansion

$$(T_n f)(z) = \sum_{m=0}^{\infty} a_m(T_n f) q^m,$$

where $a_m(T_n f) = \sum_{d | (n,m)} d^{k-1} a_{mn/d^2}((d)f)$. In particular if $f \in \mathcal{M}_k(N,\varepsilon)$, then

$$a_m(T_n f) = \sum_{d | (n,m)} \varepsilon(d) d^{k-1} a_{mn/d^2}(f)$$

For a proof see [6], Proposition 5.3.1.
1.3 The Petersson inner product

In order to define newforms, we need to put an inner product on cusp forms, as follows.

Let $H$ be the upper half plane of $\mathbb{C}$; we can define the hyperbolic measure on it, given by

$$d\mu(z) = \frac{dx \wedge dy}{y^2},$$

where $z = x + iy$. This measure is invariant under the action of the automorphism group $\text{GL}_2^+(\mathbb{R})$ of $H$, and in particular it is $\text{SL}_2(\mathbb{Z})$-invariant; indeed

$$d\mu(z) = \frac{dz \wedge d\overline{z}}{i(z - \overline{z})^2}.$$

We can compute that

$$d\mu(\gamma z) = \frac{\det \gamma}{j(\gamma, z)^2} dz, \quad d(\gamma \overline{z}) = \frac{\det \gamma}{j(\gamma, \overline{z})^2} d\overline{z}$$

and $\gamma z - \gamma \overline{z} = \frac{\det \gamma}{j(\gamma, z) j(\gamma, \overline{z})} (z - \overline{z})$, thus $d\mu(\gamma z) = d\mu(z)$.

Since the set $\mathbb{Q} \cup \{\infty\}$ is countable, its measure is 0, so we can use $d\mu$ to integrate over $H^* = H \cup \mathbb{Q} \cup \{\infty\}$. A fundamental domain of $H^*$ under the action of $\text{SL}_2(\mathbb{Z})$ is

$$D^* = D \cup \{\infty\} = \{z \in H : |\Re(z)| \leq 1/2, |z| \geq 1\} \cup \{\infty\}.$$

To show this, let us take $z \in H$ and repeatedly apply one of

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}$$

and $\overline{z}$ to translate $z$ into the vertical strip $\{|\Re(z)| \leq 1/2\}$. Now, if $z \notin D$, then $|z| < 1$ and so

$$\Im \left( -\frac{1}{z} \right) = \Im \left( -\frac{\overline{z}}{|z|^2} \right) = \Im \left( \frac{z}{|z|^2} \right) > \Im(z).$$

So we can replace $z$ by $-\frac{1}{z} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} (z)$ and repeat the process until the resulting $z$ belongs to $D$. Let us see why this process ends after a finite number of steps. We can notice that there are only finitely many matrices $\gamma \in \text{SL}_2(\mathbb{Z})$ such that $\Im(\gamma z) > \Im(z)$; it holds

$$\Im(\gamma z) = \frac{\Im(z)}{j(\gamma, z)^2}$$

and so $\Im(\gamma z) > \Im(z)$ if and only if $j(\gamma, z) < 1$. Now, there are finitely many pairs $(c, d)$ such that $|cz + d| < 1$, hence there are finitely many matrices
1.3. THE PETERSSON INNER PRODUCT

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \text{SL}_2(\mathbb{Z})$$
which increase the imaginary part. In particular, there is a matrix $\gamma$ such that $j(\gamma, z)$ is minimal, thus $\Im(\gamma z)$ is maximal; we can apply one the matrices $\begin{pmatrix} 1 & \pm 1 \\ 0 & 1 \end{pmatrix}$ a finite number of times to move $\gamma z$ into the stripe $\{|\Re(z)| < 1/2\}$, obtaining a new element $z'$ that is $\text{SL}_2(\mathbb{Z})$-equivalent to $z$. Now, if $|z'| < 1$, then $\left| \frac{-1}{z'} \right| > 1$, but $\frac{-1}{z}$ is $\text{SL}_2(\mathbb{Z})$-equivalent to $z$ and its imaginary part is greater than $\Im(\gamma z)$, a contradiction.

As for the cusps, we already know that for each $s \in \mathbb{Q}$ there exists $\gamma \in \text{SL}_2(\mathbb{Z})$ such that $\gamma s = \infty$.

Moreover for any continuous, bounded function $\phi : \mathcal{H} \to \mathbb{C}$ and any $\alpha \in \text{SL}_2(\mathbb{Z})$, the integral

$$\int_{D^*} \phi(\alpha z) d\mu(z)$$

converges. Now let $\Gamma$ be a congruence subgroup of $\text{SL}_2(\mathbb{Z})$, and let $\{\alpha_j\}_j$ be a subset of $\text{SL}_2(\mathbb{Z})$ such that the following holds:

$$\text{SL}_2(\mathbb{Z}) = \bigcup_j \left\{ \pm I \right\} \Gamma \alpha_j,$$

and the union is disjoint. Let $\phi$ be $\Gamma$-invariant. Then $\sum_j \int_{D^*} \phi(\alpha_j z) d\mu(z)$ does not depend on the choice of the representatives $\alpha_j$ and is equal to

$$\int_{\bigcup \alpha_j(D^*)} \phi(z) d\mu(z).$$

We also write $\int_{X(\Gamma)} \phi(z) d\mu(z)$ to indicate the integral above.

In particular, setting $\phi = 1$, we obtain what is called the volume of $X(\Gamma)$:

$$V_\Gamma = \int_{X(\Gamma)} d\mu(z).$$

Note that the volumes $V_\Gamma$ and $V_{\text{SL}_2(\mathbb{Z})}$ are related by the following

$$V_\Gamma = [\text{SL}_2(\mathbb{Z}) : \left\{ \pm I \right\} \Gamma] V_{\text{SL}_2(\mathbb{Z})}. \quad (1.1)$$

To construct the Petersson inner product of two cusp forms $f, g \in S_k(\Gamma)$, let

$$\phi(z) = f(z) \overline{g(z)} \Im(z)^k$$

for $z \in \mathcal{H}$.

\footnote{This notation is due to modular curves, which are not dealt with here.}
This function is continuous, being the composition of continuous functions, and $\Gamma$-invariant: for any $\gamma \in \Gamma$,
\[
\phi(\gamma z) = f(\gamma z)g(\gamma z)\Im(\gamma z)^k = j(\gamma, z)^k(f[\gamma]k(z))j(\gamma, z)^k g(\gamma z)\Im(\gamma z)^k |j(\gamma, z)|^{-2k} = (f[\gamma]k(z))(g[\gamma]k(z))\Im(z)^k = f(z)g(z)\Im(z)^k
\]
since $f$ and $g$ are $\Gamma$-invariant.

Now we need to show that such $\phi$ is bounded on $\mathbb{C}$, which reduces to show that it is bounded on $\bigcup \alpha_j(D)$. Since this union is finite, it suffices to prove that for each $\alpha \in \text{SL}_2(\mathbb{Z})$, the function $\phi \circ \alpha$ is bounded on $D$. Being continuous, it is bounded in every compact subset of $D$; near $\infty$, we can use its Fourier expansion. Remembering that
\[
(f[\alpha]k(z)) = \sum_{n=1}^{\infty} a_n(f[\alpha]k)q_n^h, \quad (g[\alpha]k(z)) = \sum_{n=1}^{\infty} a_n(g[\alpha]k)q_n^h,
\]
where $q_h = e^{2\pi i z/h}$ for some $h \in \mathbb{Z}^+$, and since $|q_h| = e^{-2\pi \Im(z)/h}$, we have that
\[
|(f[\alpha]k(z))| \cdot |(g[\alpha]k(z))| \cdot |\Im(z)|^k
\]
tends to 0 as $\Im(z) \to \infty$. Hence, the following inner product is well defined.

**Definition 1.24.** Let $\Gamma \subset \text{SL}_2(\mathbb{Z})$ be a congruence subgroup; the Petersson inner product is given by:
\[
\langle , \rangle : \mathcal{S}_k(\Gamma) \times \mathcal{S}_k(\Gamma) \to \mathbb{C}
\]
\[
(f, g) \mapsto \frac{1}{V_\Gamma} \int_{X(\Gamma)} f(z)\overline{g(z)}\Im(z)^k d\mu(z).
\]

The Petersson inner product is linear in $f$, conjugate linear in $g$, Hermitian symmetric, and positive definite. Moreover the factor $\frac{1}{V_\Gamma}$ ensures that if $\Gamma' \subseteq \Gamma$, then $\langle , \rangle_{\Gamma'} = \langle , \rangle_{\Gamma}$ on $\mathcal{S}_k(\Gamma)$.

### 1.3.1 The adjoints of Hecke operators

Using this inner product we can determine the adjoints of Hecke operators; if $T$ is one such operator, its adjoint is $T^*$ such that
\[
\langle Tf, g \rangle = \langle f, T^* g \rangle, \ \forall f, g \in \mathcal{S}_k(\Gamma_1(N)).
\]

First, we need some technical results. Let $\Gamma$ be a congruence subgroup of $\text{SL}_2(\mathbb{Z})$ and let $\{\alpha_i\}_i$ be a set of representatives of $\frac{\text{SL}_2(\mathbb{Z})}{\{\pm I\} \Gamma}$, that means such that
\[
\text{SL}_2(\mathbb{Z}) = \bigcup_i \{\pm I\} \Gamma \alpha_i;
\]
let $\alpha \in \text{GL}_2^+ (\mathbb{Q})$; then $\frac{\mathcal{H}^*}{\alpha^{-1}\Gamma\alpha} = \bigcup_i \alpha^{-1}\alpha_i(D^*)$. Defining

$$\int_{\frac{\mathcal{H}^*}{\alpha^{-1}\Gamma\alpha}} \phi(z) d\mu(z) = \sum_i \int_{D^*} \phi(\alpha^{-1}\alpha_iz) d\mu(z),$$

where $\phi : \mathcal{H} \to \mathbb{C}$ is continuous, bounded and invariant with respect to $\alpha^{-1}\Gamma\alpha$, then clearly

$$\int_{X(\Gamma)} \phi(z) d\mu(z) = \int_{\frac{\mathcal{H}^*}{\alpha^{-1}\Gamma\alpha}} \phi(\alpha z) d\mu(z).$$

Moreover, if also $\alpha^{-1}\Gamma\alpha$ is a subgroup of $\text{SL}_2(\mathbb{Z})$, then the volumes $V_{\alpha^{-1}\Gamma\alpha}$ and $V_{\Gamma}$ are equal (just set $\phi = 1$ in the equality above), and so

$$[\text{SL}_2(\mathbb{Z}) : \alpha^{-1}\Gamma\alpha] = [\text{SL}_2(\mathbb{Z}) : \Gamma],$$

which follows from Formula (1.1) and the fact that $-I \in \alpha^{-1}\Gamma\alpha$ if and only if it belongs to $\Gamma$. Hence

$$[\text{SL}_2(\mathbb{Z}) : \alpha^{-1}\Gamma\alpha \cap \Gamma] = [\text{SL}_2(\mathbb{Z}) : \Gamma \cap \alpha\Gamma\alpha^{-1}],$$

and similarly $[\Gamma : \alpha^{-1}\Gamma\alpha \cap \Gamma] = [\Gamma : \Gamma \cap \alpha\Gamma\alpha^{-1}]$. Let $n$ be this number. So there are $\gamma_1, \ldots, \gamma_n$ and $\tilde{\gamma}_1, \ldots, \tilde{\gamma}_n$ such that

$$\Gamma = \bigcup_i (\alpha^{-1}\Gamma\alpha \cap \Gamma)\gamma_i = \bigcup_i (\alpha\Gamma\alpha^{-1} \cap \Gamma)\tilde{\gamma}_i^{-1},$$

and both the unions are disjoint. We know from Lemma 1.12 applied to $\Gamma_1 = \Gamma_2 = \Gamma$ and taking respectively $\alpha$ and $\alpha^{-1}$ as the $\alpha$ in the lemma, that

$$\Gamma\alpha\Gamma = \bigcup_i \Gamma\alpha\gamma_i \quad \quad \Gamma\alpha^{-1}\Gamma = \bigcup_i \Gamma\alpha^{-1}\tilde{\gamma}_i^{-1},$$

and the latter is equivalent to $\Gamma\alpha\Gamma = \bigcup_i \tilde{\gamma}_i\alpha\Gamma$.

It is easy to see that $\Gamma\alpha\gamma_i \cap \tilde{\gamma}_i\alpha\Gamma$ is never empty: if it were, there would exist $j$ such that

$$\Gamma\alpha\gamma_j \subseteq \bigcup_{i \neq j} \tilde{\gamma}_i\alpha\Gamma,$$

thus multiplying by $\Gamma$,

$$\Gamma\alpha\Gamma \subseteq \bigcup_{i \neq j} \tilde{\gamma}_i\alpha\Gamma,$$

but this is impossible. Now, if we take $\beta_i \in \Gamma\alpha\gamma_i \cap \tilde{\gamma}_i\alpha\Gamma$ for every $i = 1, \ldots, n$, we have

$$\Gamma\alpha\Gamma = \bigcup_i \Gamma\beta_i = \bigcup_i \beta_i\Gamma.$$
Using these facts it is easy to show that given $\alpha \in \text{GL}_2^+(\mathbb{Q})$ and setting $\alpha' = \det(\alpha)\alpha^{-1}$, then if $\alpha^{-1}\Gamma\alpha \subseteq \text{SL}_2(\mathbb{Z})$ it holds
\[
\langle f[\alpha]_k, g \rangle_{\alpha^{-1}\Gamma\alpha} = \langle f(g[\alpha']_k) \rangle_{\Gamma}
\]
for every $f \in \mathcal{S}_k(\Gamma)$ and $g \in \mathcal{S}_k(\alpha^{-1}\Gamma\alpha)$.

Moreover for all $f,g \in \mathcal{S}_k(\Gamma)$,
\[
\langle f[\Gamma\alpha\Gamma]_k, g \rangle = \langle f, g[\Gamma\alpha']_k \rangle_{\Gamma}\tag{1.3}
\]

This two equalities combine to show the following theorem.

**Theorem 1.25.** In $\mathcal{S}_k(\Gamma_1(N))$, the adjoints of the Hecke operators $\langle p \rangle$ and $T_p$ for $p$ a prime number that does not divide $N$ are
\[
\langle p \rangle^* = \langle p \rangle^{-1}, \quad T_p^* = \langle p \rangle^{-1}T_p.
\]

**Proof.** Since $\Gamma_1(N)$ is normal in $\Gamma_0(N)$, if $\alpha \in \Gamma_0(N)$ has lower right entry equal to $p$ modulo $N$ then by (1.2) $\langle p \rangle^* = [\alpha]_k^* = [\alpha^{-1}]_k = \langle p \rangle^{-1}$. As for the operator $T_p$, by (1.3) we have
\[
T_p^* = \left[ \Gamma \begin{pmatrix} 0 & p \\ 1 & 0 \end{pmatrix} \Gamma \right]^* k = \left[ \Gamma \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \Gamma \right]^*_k.
\]

To compute this, we can note that
\[
\begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & n \\ N & mp \end{pmatrix}^{-1} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} p & n \\ N & m \end{pmatrix},
\]
where $mp - nN = 1$. Hence, noticing that the first matrix in the triple product lies in $\Gamma_1(N)$ while the third is in $\Gamma_0(N)$,
\[
\Gamma_1(N) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(N) = \Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \begin{pmatrix} p & n \\ N & m \end{pmatrix} \Gamma_1(N) = \\
= \Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N) \begin{pmatrix} p & n \\ N & m \end{pmatrix}.
\]

So we have that this operator is given by $T_p[\beta]_k$, where $\beta = \begin{pmatrix} p & n \\ N & m \end{pmatrix}$ has lower right entry equal to $p^{-1}$ modulo $N$, thus $T_p^* = \langle p^{-1}\rangle T_p^2$.

\footnote{Notice that even if $p^{-1}$ is not integer, it is an element of $(\mathbb{Z}/N\mathbb{Z})^*$, hence $\langle p^{-1}\rangle$ is well defined.}
Knowing this, we can compute the adjoints of Hecke operators of type \( \langle n \rangle \) and \( T_n \) for \( (n, N) = 1 \). If this condition does not hold, we can compute adjoints anyway.

As for the diamond operator, if \( (n, N) \neq 1 \) then \( \langle n \rangle = 0 \) and so \( \langle n \rangle^* = 0 \). We will now prove that for every \( n \), the adjoint of operator \( T_n \) is

\[
T_n^* = w_N T_n w_N^{-1},
\]

where \( w_N \) is the operator \( \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \). It suffices to show this property for \( n = p \) a prime number. By (1.3) we know that the adjoint of \( T_p \) is given by the double coset operator

\[
\Gamma_1(N) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(N),
\]

Let \( \gamma = \begin{pmatrix} 0 & -1 \\ N & 0 \end{pmatrix} \), with \( \gamma^{-1} = \begin{pmatrix} 0 & N^{-1} \\ -1 & 0 \end{pmatrix} \). Then the equality

\[
\gamma^{-1} \begin{pmatrix} a & b \\ Nc & d \end{pmatrix} \gamma = \begin{pmatrix} d & -c \\ -Nb & a \end{pmatrix}
\]

shows that \( \gamma^{-1} \Gamma_1(N) \gamma = \Gamma_1(N) \); moreover, using this equality we can also prove that \( \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = \gamma^{-1} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \gamma \). So

\[
\begin{pmatrix} \Gamma_1(N) \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \Gamma_1(N) \end{pmatrix}_k = \\
= \begin{pmatrix} \Gamma_1(N) \gamma^{-1} \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \gamma \Gamma_1(N) \end{pmatrix}_k = \\
= [\gamma^{-1}]_k \begin{pmatrix} \Gamma_1(N) \begin{pmatrix} 1 & 0 \\ 0 & p \end{pmatrix} \Gamma_1(N) \end{pmatrix}_k [\gamma]_k = \\
= w_N T_p w_N^{-1},
\]

and that is the adjoint of \( T_p \).

General facts of linear algebra guarantee that the space of cusp forms has an orthogonal basis of simultaneous eigenforms for the Hecke operators \( \langle n \rangle, T_n \), for \( (n, N) = 1 \), since they all commute with their adjoints.

1.4 Oldforms and newforms

We now want to study the space of cusp forms \( S_k(\Gamma_1(N)) \), splitting it into two orthogonal subspaces, namely oldforms and newforms. In order to construct them, we need a class of maps that allow us to move between cusp
forms at different levels. Let

\[ \alpha_d = \begin{pmatrix} d & 0 \\ 0 & 1 \end{pmatrix} \]

be the multiplication by \( d \). If \( M \mid N \) and \( d \mid \frac{N}{M} \), then the map \( f \mapsto f[\alpha_d]_k \) takes \( S_k(\Gamma_1(M)) \) to \( S_k(\Gamma_1(N)) \).

For each divisor \( d \) of \( N \), let us consider the map \( i_d \) given by

\[ i_d : S_k(\Gamma_1(Nd^{-1})) \times S_k(\Gamma_1(Nd^{-1})) \to S_k(\Gamma_1(N)) \]
\[ (f, g) \mapsto f + g[\alpha_d]_k. \]

**Definition 1.26.** The subspace of oldforms at level \( N \) is

\[ S_k(\Gamma_1(N))^{\text{old}} = \sum_{p \mid N, \text{ prime}} \text{Im}(i_p). \]

The subspace of newforms at level \( N \) is the orthogonal complement of oldforms with respect to the Petersson inner product,

\[ S_k(\Gamma_1(N))^{\text{new}} = (S_k(\Gamma_1(N))^{\text{old}}) ^\perp. \]

The Hecke operators respect the decomposition into oldforms and newforms, as shown in the following proposition.

**Proposition 1.27.** The subspaces \( S_k(\Gamma_1(N))^{\text{old}} \) and \( S_k(\Gamma_1(N))^{\text{new}} \) are stable under the Hecke operators \( T_n \) and \( \langle n \rangle \) for every \( n \in \mathbb{Z}^+ \).

**Proof.** Let us first consider oldforms; by definition, an oldform is an element of

\[ \sum_{p \mid N, \text{ prime}} i_p(S_k(\Gamma_1(Np^{-1})) \times S_k(\Gamma_1(Np^{-1}))). \]

Let \( p \) be a prime dividing \( N \) and let \( T \) be a Hecke operator. We will now prove that if \( f, g \in S_k(\Gamma_1(Np^{-1})) \), then \( T \circ i_p(f, g) \) is an element in \( \text{Im}(i_p) \).

If \( T \) is the diamond operator \( \langle d \rangle \) we have two cases: if \( (d, N) \neq 1 \), then \( \langle d \rangle = 0 \) and clearly 0 is an oldform; if otherwise \( (d, N) = 1 \), then let \( \alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \) be a matrix representing \( \langle d \rangle \), where \( d \equiv d \pmod{N} \); then

\[ \langle d \rangle \circ i_p(f, g) = \langle d \rangle(f + g[\alpha_p]_k) = \langle d \rangle f + g[\alpha_p\alpha]_k. \]

It is an easy calculation to check that \( \alpha_p\alpha = \alpha'\alpha_p \), where

\[ \alpha' = \begin{pmatrix} a & pb \\ cp^{-1} & \delta \end{pmatrix}. \]
represents the operator $\langle d \rangle$ on $\Gamma_1(Np^{-1})$. Hence

$$\langle d \rangle f + g[\alpha_p \alpha]_k = \langle d \rangle f + g[\alpha \alpha_p]_k = i_p(\langle d \rangle f + g[\alpha'])_k.$$  

Now, let $p' \neq p$ be another prime number. Then

$$T_{p'} g = \begin{cases}
\sum_{i=0}^{p'-1} g \left[ \begin{pmatrix} 1 & i \\ 0 & p' \end{pmatrix} \right]_k & p' \mid N \\
\sum_{i=0}^{p'-1} g \left[ \begin{pmatrix} 1 & i \\ 0 & p' \end{pmatrix} \right]_k + g \left[ \begin{pmatrix} m & n \\ N & p' \end{pmatrix} \begin{pmatrix} p' & 0 \\ 0 & 1 \end{pmatrix} \right]_k & p' \nmid N,
\end{cases}$$  

where in the second equality $mp' - nN = 1$. By direct calculation,

$$\left( \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & i \\ 0 & p' \end{pmatrix} \right) = \left( \begin{pmatrix} 1 & ip \\ 0 & p' \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right),$$

and since the numbers $\{ip : i = 0, \ldots, p' - 1\}$ represent all the elements of $\mathbb{Z}_{p'/\mathbb{Z}}$, it holds

$$\left( \sum_{i=0}^{p'-1} g \left[ \begin{pmatrix} 1 & i \\ 0 & p' \end{pmatrix} \right]_k \right)[\alpha_p]_k = \sum_{i=0}^{p'-1} g[\alpha_p]_k \left[ \begin{pmatrix} 1 & i \\ 0 & p' \end{pmatrix} \right]_k.$$

If $p' \nmid N$, we also need to consider the additional term in the second equality; we can note that

$$\left( \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} m & n \\ N & p' \end{pmatrix} \begin{pmatrix} p' & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right),$$

and the matrix $\left( \begin{pmatrix} m & np \\ Np^{-1} & p' \end{pmatrix} \begin{pmatrix} p' & 0 \\ 0 & 1 \end{pmatrix} \right)$ represents the additional term in $T_{p'} g$ at level $Np^{-1}$. Hence $T_{p'}$ and $i_p$ commute, precisely

$$T_{p'} \circ i_p(f, g) = i_p(T_{p'} f, T_{p'} g)$$

and so $T_{p'}$ takes oldforms to oldforms. Let us consider $T_p$. We claim that

$$T_p \circ i_p(f, g) = i_p(T_p f + p^{k-1} g, -(p)f).$$

Let us first suppose that $p^2 \nmid N$. Then,

$$i_p(T_p f + p^{k-1} g, -(p)f) = \sum_{i=0}^{p-1} f \left[ \begin{pmatrix} 1 & i \\ 0 & p \end{pmatrix} \right]_k + f \left[ \begin{pmatrix} m & np \\ Np^{-1} & p \end{pmatrix} \right]_k + p^{k-1} g - f[\alpha \alpha_p]_k,$$
where \( \alpha \) represents the diamond operator \( \langle p \rangle \). Choosing \( \alpha \equiv \left( \frac{mp^{-1}}{Np^{-2}} \frac{np}{p} \right) \) (mod \( Np^{-1} \)) - note that all this numbers exist in \( \mathbb{Z}_{Np^{-1}} \mathbb{Z} \), under the assumption \( p^2 \nmid N \) - the two terms \( f \left[ \left( \frac{m}{Np^{-1}} \frac{np}{p} \right) \right] \) and \( f[\alpha \alpha] \) are equal and so drop out, giving \( i_p(T_pf + p^{k-1}g, -(p)f) = \sum_{i=0}^{p-1} f \left[ \left( \frac{1}{0} \frac{i}{p} \right) \right] + p^{k-1}g. \)

On the other hand,

\[
T_p \circ i_p(f, g) = \sum_{i=0}^{p-1} f \left[ \left( \frac{1}{0} \frac{i}{p} \right) \right] + \sum_{i=0}^{p-1} g \left[ \alpha_p \left( \frac{1}{0} \frac{i}{p} \right) \right],
\]

so we need to compute this last term. First we note that \( \alpha_p \left( \frac{1}{0} \frac{i}{p} \right) = pI \circ \left( \frac{1}{0} \frac{i}{1} \right) \); we have

\[
g \left[ pI \circ \left( \frac{1}{0} \frac{i}{1} \right) \right] = g[pI]_k \left[ \left( \frac{1}{0} \frac{i}{1} \right) \right] = p^{k-2}g \left[ \left( \frac{1}{0} \frac{i}{1} \right) \right] = p^{k-2}g;
\]

so \( T_p \circ i_p(f, g) = \sum_{i=0}^{p-1} f \left[ \left( \frac{1}{0} \frac{i}{p} \right) \right] + p^{k-1}g \), as wanted.

Finally, if \( p^2 \mid N \), the operator \( \langle p \rangle \) is 0 and \( i_p(T_pf + p^{k-1}g, -(p)f) = \sum_{i=0}^{p-1} f \left[ \left( \frac{1}{0} \frac{i}{p} \right) \right] + p^{k-1}g = T_p \circ i_p(f, g) \) as before. So far, we have considered all the possible Hecke operators and hence proved that oldforms are stable under them. As for newforms, we proceed as follows. If \( f \) is a newform, \( g \) is an oldform and \( T \) is a Hecke operator, then

\[
\langle f, T^* g \rangle = \langle T f, g \rangle;
\]

if \( T^* g \) is still an oldform, then the inner product above is equal to 0, hence \( Tf \) is a newform as well. So we just need to show that oldforms are stable under the adjoints of Hecke operators. The adjoint of a diamond operator is another diamond operator, so there is nothing to show. Moreover, we know from previous section that \( T^*_n = w_N T_n w_N^{-1} \), where \( w_N = \left[ \begin{array}{cc} 0 & 1 \\ -N & 0 \end{array} \right] \).

Then it suffices to show that this last operator preserves oldforms; to do so,
we claim that \( w_N \circ i_p(f, g) = i_p(p^{k-2}w_{N^p-1}g, w_{N^p-1}f) \). It holds:

\[
i_p(p^{k-2}w_{N^p-1}g, cw_{N^p-1}f) = \quad i_p \left( p^{k-2}g \begin{pmatrix} 0 & 1 \\ -Np^{-1} & 0 \end{pmatrix}_k, f \begin{pmatrix} 0 & 1 \\ -Np^{-1} & 0 \end{pmatrix}_k \right) = p^{k-2}g \begin{pmatrix} 0 & 1 \\ -Np^{-1} & 0 \end{pmatrix}_k + f \begin{pmatrix} 0 & 1 \\ -Np^{-1} & 0 \end{pmatrix}_k \left( \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} \right)_k;\]
on the other hand

\[
w_N \circ i_p(f, g) = f \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}_k + g \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}_k \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}_k.\]

Direct calculation shows that \( \begin{pmatrix} 0 & 1 \\ -Np^{-1} & 0 \end{pmatrix} \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix} \), and so the terms involving \( f \) are the same in the two expressions, and

\[
p^{k-2}g \begin{pmatrix} 0 & 1 \\ -Np^{-1} & 0 \end{pmatrix}_k(z) = (-1)^{-k}N^{-1}p^{k-1}z^{-k}g \left( \frac{-p}{Nz} \right);\]

\[
g \begin{pmatrix} p & 0 \\ 0 & 1 \end{pmatrix}_k \begin{pmatrix} 0 & 1 \\ -N & 0 \end{pmatrix}_k = (-1)^{-k}N^{-1}p^{k-1}z^{-k}g \left( \frac{-p}{Nz} \right).\]

This concludes the proof. \( \square \)

In particular the spaces \( \mathcal{S}_k(\Gamma_1(N))^{\text{old}} \) and \( \mathcal{S}_k(\Gamma_1(N))^{\text{new}} \) have orthogonal bases of eigenforms for the Hecke operators \( (n) \) and \( T_n \) with \( (n, N) = 1 \).

### 1.4.1 Eigenforms

This section uses a theorem due to Atkin and Lehner; we omit the proof, which can be found in [6] (see Theorem 5.7.1), and use it to prove some basic properties of newforms. Note that in this section the meaning of the term newform will be slightly different from that in the previous section, as will be specified in Definition 1.29.

**Theorem 1.28 (Atkin-Lehner).** If \( f \in \mathcal{S}_k(\Gamma_1(N)) \) has Fourier expansion

\[
f(z) = \sum_n a_n(f)q^n, \quad q = e^{2\pi iz/N}\]

with \( a_n(f) = 0 \) whenever \( (n, N) = 1 \), then \( f \) takes the form

\[
f = \sum_{p|N} \iota_p f_p\]

with each \( f_p \in \mathcal{S}_k(\Gamma_1(Np^{-1})) \); the map \( \iota_p \) is defined as follows:

\[
\iota_p = p^{1-k}[\alpha_p]_k : \mathcal{S}_k(\Gamma_1(Np^{-1})) \rightarrow \mathcal{S}_k(\Gamma_1(N)).\]
We already know that the spaces \((S_k(\Gamma_1(N)))^{\text{old}}\) and \((S_k(\Gamma_1(N)))^{\text{new}}\) have orthogonal bases of eigenforms for the Hecke operators \(\langle n \rangle\) and \(T_n\) with \((n, N) = 1\). Our aim is now to show that if \(f\) is an element of such a basis for \((S_k(\Gamma_1(N)))^{\text{new}}\), then it is an eigenform for all Hecke operators. In the case of the diamond operator, there is nothing to show: if \((n, N) \neq 1\), then \(\langle n \rangle\) is simply the zero operator and clearly \(f\) is an eigenform for it.

We shall now consider Hecke operators of the second type.

**Definition 1.29.** A nonzero modular form \(f \in M_k(\Gamma_1(N))\) that is an eigenform for all the Hecke operators is a (Hecke) eigenform. The Hecke eigenform

\[
f(z) = \sum_{n=0}^{\infty} a_n(f) q^n, \quad q = e^{2\pi iz/N}
\]

is normalized when \(a_1(f) = 1\). A newform is a normalized Hecke eigenform in \((S_k(\Gamma_1(N)))^{\text{new}}\).

The following theorem will prove our statement and give a relation between the eigenvalues of Hecke operators and Fourier coefficients.

**Theorem 1.30.** Let \(f \in (S_k(\Gamma_1(N)))^{\text{new}}\) be a nonzero eigenform for the Hecke operators \(T_n\) and \(\langle n \rangle\) for all \(n\) with \((n, N) = 1\). Then

- \(f\) is a Hecke eigenform; a suitable scalar of \(f\) is a newform;
- if \(\tilde{f}\) satisfies the same conditions as \(f\) and has the same \(T_n\)-eigenvalues, then \(\tilde{f} = cf\) for some constant \(c\).

The set of newforms in the space \((S_k(\Gamma_1(N)))^{\text{new}}\) is an orthogonal basis of it. Each such newform lies in a space \(S_k(N, \varepsilon)\) and satisfies \(T_n f = a_n(f) f\) for all \(n \in \mathbb{Z}^+\): the Fourier coefficients of \(f\) are its \(T_n\)-eigenvalues.

**Proof.** Let \(f \in S_k(\Gamma_1(N))\) be an eigenform for \(T_n\) and \(\langle n \rangle\) where \((n, N) = 1\); thus there exist some eigenvalues \(c_n\) and \(d_n \in \mathbb{C}\) such that

\[
T_n f = c_n f \quad \langle n \rangle f = d_n f
\]

for every such \(n\). The map \(n \mapsto d_n\) defines a Dirichlet character \(\varepsilon\), being a homomorphism, and so \(f \in S_k(N, \varepsilon)\). Now, using the formulas in Proposition 1.23 we can compute that \(a_1(T_n f) = a_n(f)\) for \(n \in \mathbb{Z}^+\). On the other hand, for \((n, N) = 1\), it holds \(a_1(T_n f) = c_n a_1(f)\), hence

\[
a_n(f) = c_n a_1(f) \text{ for } (n, N) = 1.
\]

In particular, if \(a_1(f) = 0\), then \(a_n(f) = 0\) for all \(n\) such that \((n, N) = 1\), and so \(f \in (S_k(\Gamma_1(N)))^{\text{old}}\) by Atkin and Lehner’s Theorem. Hence if \(f \in \)
In this final section, we will introduce Eisenstein series, which can be viewed as a complement to cusp forms in the space of modular forms. Extending the Petersson inner product to each pair of modular forms \((f, g)\) such that the integral
\[
\int_{X(\Gamma)} f(z) \overline{g(z)} \Im(z)^k d\mu(z)
\]
converges, we will be able to prove that Eisenstein series and cusp forms are orthogonal.  

1.5. Eisenstein series

\((\mathcal{S}_k(\Gamma_1(N)))^{new}\) then \(a_1(f) \neq 0\) and we may assume it is equal to 1, so that \(f\) is normalized. For \(m \in \mathbb{Z}^+\), let
\[
g_m = T_m f - a_m(f) f.
\]
This element belongs to \((\mathcal{S}_k(\Gamma_1(N)))^{new}\) and by direct calculation it is an eigenform for \(T_n\) and \(\langle n \rangle\) with \((n, N) = 1\), indeed
\[
T_n(g_m) = T_n T_m f - T_n a_m(f) f = T_m T_n f - a_m(f) T_n f = c_n g_m,
\]
\[
\langle n \rangle(g_m) = \langle n \rangle T_m f - \langle n \rangle a_m(f) f = T_m d_n f - a_m(f) d_n f = d_n g_m.
\]
Moreover \(a_1(g_m) = a_1(T_m f) - a_1(a_m(f) f) = a_m(f) - a_m(f) a_1(f) = a_m(f) - a_m(f) = 0\). Hence \(g_m \in (\mathcal{S}_k(\Gamma_1(N)))^{new} \cap (\mathcal{S}_k(\Gamma_1(N)))^{old} = \{0\}\). This proves that \(T_m f = a_m(f) f\) for every \(m \in \mathbb{Z}^+\), hence \(f\) is a Hecke eigenform (a newform if we normalize it), with eigenvalues for the operators \(T_n\) given by its Fourier coefficients; if \(\tilde{f}\) satisfies the same conditions as \(f\) and has the same eigenvalues, then the Fourier coefficients of \(f\) and \(\tilde{f}\) only differ by a constant. To prove that the set of newforms is an orthogonal basis of \((\mathcal{S}_k(\Gamma_1(N)))^{new}\) we just need to show that it is linearly independent. Let by contradiction
\[
\sum_{i=1}^n c_i f_i = 0
\]
for some \(c_i \in \mathbb{C}\), all different from 0, with as few terms as possible (in particular \(n \geq 2\)). Then for any prime \(p\), applying \(T_p - a_p(f_1)\) to the relation gives
\[
\sum_{i=2}^n c_i (a_p(f_1) - a_p(f_i)) f_i = 0;
\]
this linear relation involves \(n - 1\) elements, so it must be 0, thus \(a_p(f_i) = a_p(f_1)\) for every \(i\). Since \(p\) is arbitrary, this gives \(f_i = f_1\) for all \(i\), and this is a contradiction since the original relation involved at least two terms. \(\square\)
Definition 1.31. An Eisenstein series with parameter associated to the congruence group \( \Gamma(N) \) is a function
\[
E_k^\bar{v}(z, s) = \epsilon_N \sum_{\gamma \in \Gamma(N) \backslash \Gamma} \Im(z)^s[\gamma]_k, \quad \Re(k + 2s) > 2,
\]
where:

- \( \epsilon_N = 1/2 \) if \( N = 1, 2 \) and 1 if \( N > 2 \);
- \( \bar{v} = (c_v, d_v) \in (\mathbb{Z}/N\mathbb{Z})^2 \), of order \( N \);
- \( \delta \) is a matrix in \( \text{SL}_2(\mathbb{Z}) \) whose bottom row is a lift of \( \bar{v} \) to \( \mathbb{Z}^2 \);
- \( P_+ \) is the subgroup of \( \text{SL}_2(\mathbb{Z}) \) consisting of the matrices \( \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \), \( n \in \mathbb{Z} \).

Here, the weight-\( k \) operators act on the function \( \Im(z)^s \), which depends on two parameters, and is defined, in general, as
\[
f[\gamma]_k(z, s) = j(\gamma, z)^{-k} f(\gamma z, s).
\]

We can analytically continue the function \( E_k^\bar{v}(z, s) \) at \( s = 0 \), though not necessarily obtaining a holomorphic function: for example at weight \( k = 2 \) the continued series is nonholomorphic, but linear combinations cancel away the nonholomorphic terms. Hence we can give the following definition.

Definition 1.32. The Eisenstein space with respect to \( \Gamma(N) \) is the subspace \( \mathcal{E}_k(\Gamma(N)) \) of \( \mathcal{M}_k(\Gamma(N)) \) given by the holomorphic functions in
\[
\text{Span} \left\{ E_k^\bar{v}(z, 0) : \bar{v} \in \left( \mathbb{Z}/N\mathbb{Z} \right)^2, \text{ord}(\bar{v}) = N \right\}.
\]

It can be shown that this space is isomorphic to the quotient \( \mathcal{M}_k(\Gamma(N)) / \mathcal{S}_k(\Gamma(N)) \) (see [6], §5.11) hence we can write
\[
\mathcal{M}_k(\Gamma(N)) \cong \mathcal{S}_k(\Gamma(N)) \oplus \mathcal{E}_k(\Gamma(N)).
\]

Eisenstein series as defined here are the general case of classical Eisenstein series, which are
\[
G_k(z) = \sum_{(c,d) \in \mathbb{Z}^2 \backslash \{(0,0)\}} (cz + d)^{-k};
\]
the series \( G_k \) is called Eisenstein series of weight \( k \).
Moreover, as mentioned at the beginning of this section, cusp forms and Eisenstein series are orthogonal with respect to the Petersson inner product. To show this we will first need some notation. Let $P^+(N) = P_+ \cap \Gamma(N)$, $D_N^*$ be a fundamental domain for the orbit space $\frac{H^*}{P_+(N)}$, where

$$D_N^* = \{ z \in H^* \cap \mathbb{C} : 0 \leq \Re(z) \leq N \} \cup \{ \infty \}.$$ 

Now let $\alpha_i, \beta_j$ satisfy $\Gamma(N) P_+ = \bigcup_i P_+(N) \alpha_i$ and $\frac{\text{SL}_2(\mathbb{Z})}{\Gamma(N)} = \bigcup_j \Gamma(N) \beta_j$, so that $\text{SL}_2(\mathbb{Z}) P_+ = \bigcup_{i,j} P_+(N) \alpha_i \beta_j$, $D_N^* = \bigcup_{i,j} \alpha_i \beta_j(D^*)$.

If $f$ is a cusp form in $S_k(\Gamma(N))$, then the condition $a_0(f) = 0$ implies that

$$\int_0^N f(x + iy)dx = 0$$

for $y > 0$ and so for any $s \in \mathbb{C}$ such that $\Re(k + 2s) \geq 0$ it holds

$$\int_{y=0}^\infty \int_{x=0}^N f(x + iy)y^{k+s-2}dxdy = 0,$$

that can be re-written as

$$\int_{D_N^*} f(z) \Im(z)^{k+s}d\mu(z);$$

it follows

$$0 = \sum_{i,j} \int_{D^*} f(\alpha_i \beta_j z) \Im(\alpha_i \beta_j z)^{k+s}d\mu(z) =$$

$$= \sum_{i,j} \int_{D^*} f(\beta_j z) j^{\alpha_i} \beta_j z^k \Im(\beta_j z)^{k+s} |j(\alpha_i, \beta_j z)|^{2(k+s)}d\mu(z) =$$

$$= \sum_j \int_{D^*} f(\beta_j z) E^{(0,1)}_k(\beta_j z, s)/\epsilon_N \Im(\beta_j z)^{k}d\mu(z),$$

where the last equality holds when $\Re(k + 2s) > 2$ (in which case the sum over $i$ converges absolutely and passes through the integral). In particular, this shows that the Petersson inner product of $f(z)$ and $E^{(0,1)}_k(z, s)$ is 0 for all $s$ such that $\Re(k + 2s) > 2$. This relation analytically continues to $s = 0$, giving

$$\langle f, E^{(0,1)}_k \rangle = 0.$$
Now, for $\bar{v} \in \left( \frac{Z}{NZ} \right)^2$ of order $N$, there is $\gamma \in \text{SL}_2(Z)$ such that $\bar{v} = (0, 1)\gamma$. So, for any cusp form $f \in S_k(\Gamma(N))$:

$$\langle f, E_k^{(0,1)}(0,1) \Gamma(N) \rangle = \langle f, E_k^{(0,1)}[\gamma] \Gamma(N) \rangle = \langle f[\gamma^{-1}]_k, E_k^{(0,1)} \Gamma(N) \rangle,$$

where the last equality follows from Formula (1.2). Since also $f[\gamma^{-1}]_k$ is a cusp form, $\langle f, E_k^{(0,1)}(0,1) \Gamma(N) \rangle = 0$. This proves that Eisenstein series as here defined and cusp forms are orthogonal. For any congruence subgroup $\Gamma$ of $\text{SL}_2(Z)$ at level $N$ we define

$$E_k(\Gamma) = E_k(\Gamma(1)) \cap M_k(\Gamma)$$

and for a Dirichlet character $\varepsilon$ modulo $N$:

$$E_k(N, \varepsilon) = E_k(\Gamma(1)) \cap M_k(N, \varepsilon).$$

In particular, this proves that any modular form is the sum of an Eisenstein series and a cusp form. Our main concern about Eisenstein series is the following theorem, which will be used in the proof of Deligne-Serre’s Theorem.

**Theorem 1.33.** Let $N \in Z^+$ and let $A_{N,1}$ be the set of all $(\{\psi, \varphi\}, t)$ such that $\psi$ and $\varphi$ are Dirichlet character modulo $u, v$ respectively, with $uv | N$, $\psi \varphi$ is odd, and $t \in Z^+$ is such that $tuv | N$. Set

$$E_{1,1}^{\{\psi, \varphi\}}(z) = \delta(\varphi)L(0, \psi) + \delta(\psi)L(0, \varphi) + 2 \sum_{n=1}^{\infty} \sigma_0^{\{\psi, \varphi\}}(n)e^{2\pi i nz},$$

where

- $\delta(\varphi) = 1$ if $\varphi$ is trivial, 0 otherwise;
- $L(s, \varphi)$ is the Dirichlet series associated to $\varphi$, namely
  $$L(s, \varphi) = \sum_{n=1}^{\infty} \varphi(n) n^{-s};$$
- $\sigma_0^{\{\psi, \varphi\}}(n) = \sum_{m|n} \psi(n/m)\varphi(m)$.

If we also set $E_{1,1}^{\{\psi, \varphi\}, t}(z) = E_{1,1}^{\{\psi, \varphi\}}(tz)$, then the set of all $E_{1,1}^{\{\psi, \varphi\}, t}$ forms a basis of the space $E_1(\Gamma(1)(N))$; for any character $\varepsilon$ modulo $N$, the set of the $E_{1,1}^{\{\psi, \varphi\}, t}$ with $\psi \varphi = \varepsilon$ is a basis of $E_1(N, \varepsilon)$. Finally, if $p | N$ is prime, then

$$T_p E_{1,1}^{\{\psi, \varphi\}, t} = (\psi(p) + \varphi(p)) E_{1,1}^{\{\psi, \varphi\}, t} \quad \forall E_{1,1}^{\{\psi, \varphi\}, t}.$$

This is a particular form of a more general theorem, which can be found in [6] (see Theorems 4.5.2, 4.6.2 and 4.8.1.).
Chapter 2

Deligne-Serre’s Theorem

In this chapter, we introduce Galois representations, and then we will state and prove Deligne-Serre’s Theorem.

Let \( \bar{\mathbb{Q}} \) be an algebraic closure of \( \mathbb{Q} \) and let \( G = \text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}) \) the Galois group of the (infinite) field extension \( \bar{\mathbb{Q}}/\mathbb{Q} \), that is called absolute Galois group. Let \( K \) be one of the following fields:

- the field \( \mathbb{C} \), with the discrete topology;
- a finite field, with the discrete topology;
- a \( \ell \)-adic field, where \( \ell \) is a prime number, with its natural topology, which is to be explained later.

**Definition 2.1.** A Galois representation is a linear representation of \( G \), i.e. a continuous homomorphism

\[
\rho : G \to \text{GL}_d(K),
\]

where \( K \) is as above.

2.1 A review of Number Theory

Before defining the \( \ell \)-adic topology, we will summarize some of the basic properties of \( \ell \)-adic integers and \( \ell \)-adic fields. What is stated in the following section can be found in [1], §1.

Let us consider the sequences

\[
(a_1, a_2, a_3, \ldots) : a_n \in \frac{\mathbb{Z}}{\ell^n \mathbb{Z}}, \ a_{n+1} \equiv a_n \pmod{\ell^n} \ \forall n;
\]

these form a ring, which is isomorphic to the inverse limit of \( \frac{\mathbb{Z}}{\ell^n \mathbb{Z}} \), for \( n \in \mathbb{Z}^+ \).
CHAPTER 2. DELIGNE-SERRE’S THEOREM

Definition 2.2. Let $\ell$ be a prime; an $\ell$-adic integer is an element of the ring

$$\mathbb{Z}_\ell = \lim_{\leftarrow n} \frac{\mathbb{Z}}{\ell^n \mathbb{Z}}.$$  

The ring $\mathbb{Z}_\ell$ is an integral domain; it contains $\mathbb{Z}$ as a subring, via the inclusion

$$\mathbb{Z} \to \mathbb{Z}_\ell, \quad a \mapsto (a + \ell \mathbb{Z}, a + \ell^2 \mathbb{Z}, a + \ell^3 \mathbb{Z}, \ldots);$$

this map induces an isomorphism between $\frac{\mathbb{Z}}{\ell \mathbb{Z}}$ and $\frac{\mathbb{Z}}{\mathbb{Z}}$. The units of $\mathbb{Z}_\ell$ are the group $\mathbb{Z}_\ell^*$ consisting of the sequences $(a_n)_n$ such that every $a_n \in \left(\frac{\mathbb{Z}}{\ell^n \mathbb{Z}}\right)^*$; in other words, every element $(a_n)_n$ with $a_1 \neq 0$ is invertible. The ring $\mathbb{Z}_\ell$ is local and its only maximal ideal is hence $\ell \mathbb{Z}_\ell$.

We can put a topology on $\mathbb{Z}_\ell$ as follows; let

$$U_x(n) = x + \ell^n \mathbb{Z}_\ell, \quad x \in \mathbb{Z}_\ell, \quad n \in \mathbb{Z}^+;$$

then $U_x(n)$ is a set containing $x$ and $U_x(n) \supseteq U_x(m)$ whenever $n < m$. If $x = 1$, we usually write $U(n)$ instead of $U_1(n)$. We declare that a basis for the topology on $\mathbb{Z}_\ell$ is $\{U_x(n) : x \in \mathbb{Z}_\ell, n \in \mathbb{Z}^+\}$.

We can also consider the product space $\mathbb{Z}_\ell^d$ with the product topology; a basis for it is given by

$$\{U_v(n) : v \in \mathbb{Z}_\ell^d, n \in \mathbb{Z}^+\},$$

where $U_v(n) = v + n \mathbb{Z}_\ell^d$. It is easy to see that the ring operations on $\mathbb{Z}_\ell$ are continuous with respect to this topology; moreover $\mathbb{Z}_\ell$ is compact.

Definition 2.3. The quotient field of $\mathbb{Z}_\ell$ is the field $\mathbb{Q}_\ell$ of $\ell$-adic numbers.

The field $\mathbb{Q}_\ell$ is a topological space as well, a basis for its topology being $\{U_x(n) = x + \ell^n \mathbb{Z}_\ell, x \in \mathbb{Q}_\ell, n \in \mathbb{Z}^+\}$. The field operations are continuous and as before the $\mathbb{Q}_\ell$-vector space $\mathbb{Q}_\ell^d$ is a topological space with the product topology; in particular, the matrix group $\text{GL}_d(\mathbb{Q}_\ell)$ acquires a topology being a subspace of $\mathbb{Q}_\ell^{d^2}$. Another continuous operation is the vector-by-matrix multiplication

$$\mathbb{Q}_\ell^d \times \text{GL}_d(\mathbb{Q}_\ell) \to \mathbb{Q}_\ell^d;$$

note that we are considering vectors as rows and matrices multiply from the right.

Remark 2.4. If $V$ is a finite-dimensional space over $\mathbb{Q}_\ell$, any basis of $V$ determines a topology, which is independent of the coordinates.
2.1. A REVIEW OF NUMBER THEORY

Let $B = (\beta_1, \ldots, \beta_d)$ be a basis of $V$, then it determines a topology $T$ such that the coordinate map

$$c_B : V \rightarrow \mathbb{Q}^d$$

$$\sum_i a_i \beta_i \mapsto (a_1, \ldots, a_d)$$

is a homeomorphism. If $B'$ is another basis, determining the topology $T'$, then the identity map: $(V, T) \rightarrow (V, T')$ is given by the composition $c_B^{-1} \circ m \circ c_B$, where $m$ is the matrix that expresses the transition between the bases on $\mathbb{Q}^d$. Since this is a homeomorphism, the two topologies are the same.

A number field is a field $K \subseteq \overline{\mathbb{Q}}$ such that the degree $[K : \mathbb{Q}]$ is finite. Each number field has its ring of algebraic integers (the elements of $\mathbb{Q}$ which satisfy a monic polynomial equation with coefficient in $\mathbb{Z}$), namely $\mathcal{O}_K$. If the field extension $K/\mathbb{Q}$ is Galois, and $p \in \mathbb{Z}$ is prime, then there exist positive integers $r, e, f$ such that the ideal $p\mathcal{O}_K$ is expressed as a product of maximal ideals of $\mathcal{O}_K$ as follows:

$$p\mathcal{O}_K = (p_1 \cdots p_r)^e,$$

and $\frac{\mathcal{O}_K}{p_i} \cong \mathbb{F}_{p_i}$ for $i = 1, \ldots, r$. It also holds $[K : \mathbb{Q}] = efr$.

Given a maximal ideal $\mathfrak{p}$ which lies above $p$, i.e. occurs in the factorization of $p\mathcal{O}_K$, the number $e$ is called ramification index of $\mathfrak{p}$ over $p$. There are only finitely many primes $p \in \mathbb{Z}$ such that $e > 1$, or such that $p$ ramify in $K$. The number $f$ is called the residue degree of $\mathfrak{p}$ over $p$ and is the dimension of the residue field $\frac{\mathcal{O}_K}{\mathfrak{p}}$ as a vector space over $\mathbb{F}_p$. The number $r$ is the decomposition index and is the number of distinct $\mathfrak{p}$ lying over $p$. These integers are also equal to the indices of two groups related to a Galois field extension, namely the decomposition group and the inertia group.

**Definition 2.5.** Given $K$ a Galois number field, let $p$ be a rational prime and $\mathfrak{p}$ a maximal ideal of $\mathcal{O}_K$ lying above $p$; the decomposition group of $\mathfrak{p}$ is the subgroup of the Galois group $\text{Gal}(K/\mathbb{Q})$ which fixes $\mathfrak{p}$ as a set:

$$D_p = \{ \sigma \in \text{Gal}(K/\mathbb{Q}) : p^\sigma = p \}. $$

Hence the decomposition group acts on the residue field $\frac{\mathcal{O}_K}{\mathfrak{p}}$; the kernel of this action is the inertia group:

$$I_p = \{ \sigma \in D_p : x^\sigma \equiv x \pmod{\mathfrak{p}} \forall x \in \mathcal{O}_K \}.$$ 

\[1\text{They are exactly the primes } p \text{ which divide the discriminant of the field extension } K/\mathbb{Q}.\]
The decomposition group has order $ef$; since $|\text{Gal}(K/Q)| = efr$, it means that the index of the decomposition group in the Galois group is equal to $r$. The inertia group has order $e$. So, if a prime number $p$ has only one $p$ lying above it, the decomposition group is the Galois group of the field extension. If a prime is unramified, the inertia group is trivial.

Let us write $O_K^p = F_{p^f}$. Since it is a finite field of characteristic $p$, the following automorphism is defined on it:

$$\sigma_p : x \mapsto x^p.$$  

This is called Frobenius automorphism and is a generator of the Galois group $\text{Gal}(F_{p^f}/F_p)$. There is an injection

$$\frac{D_p}{I_p} \hookrightarrow \text{Gal}(F_{p^f}/F_p).$$

Both these groups have order $f$, so this injection is in fact an isomorphism; in particular the group $\frac{D_p}{I_p}$ has a generator that maps to the Frobenius $\sigma_p$.

**Definition 2.6.** Any representative in $D_p$ of the generator of $\frac{D_p}{I_p}$ that maps to $\sigma_p$ is called a Frobenius element of $\text{Gal}(K/Q)$ and denoted $\text{Frob}_p$; it satisfies the relation

$$x^{\text{Frob}_p} \equiv x^p \pmod p \quad \forall x \in O_K.$$

If $K/Q$ is Galois then the Galois group acts transitively on the maximal ideals of $O_K$ lying above a given prime $p$. The associated decomposition and inertia groups are related by

$$D_p^\sigma = \sigma D_p \sigma^{-1}, \quad I_p^\sigma = \sigma I_p \sigma^{-1},$$  

hence $\text{Frob}_p^\sigma = \sigma \text{Frob}_p \sigma^{-1}$.

Now let $K$ be any number field and let $O_K$ be its ring of integers. Given $\ell$ a rational prime, we can write

$$\ell O_K = \prod_{\lambda | \ell} \lambda^{e_\lambda},$$  

where the notation $\lambda | \ell$ means that $\lambda$ lies above $\ell$. If $K/Q$ is not Galois, the maximal ideals $\lambda$ lying above $\ell$ may have different ramification indices $e_\lambda$.

We can define the $\lambda$-adic integers as the inverse limit

$$O_{K,\lambda} = \lim_{\leftarrow n} \frac{O_K}{\lambda^n}.$$
2.1. A REVIEW OF NUMBER THEORY

and the field of $\lambda$-adic numbers is $K_\lambda$. The residue degree is defined as $\left[ \frac{O_K}{\lambda} : \mathbb{F}_\ell \right]$. Then $\mathbb{Z}_\ell \subseteq O_{K,\lambda}$, $Q_\ell \subseteq K_\lambda$ and $[K_\lambda : Q_\ell] = e_\lambda f_\lambda$. In particular $K_\lambda$ is a finite extension of $Q_\ell$, hence it acquires a topology as a finite-dimensional vector space over $Q_\ell$. If $V$ is a finite-dimensional vector space over $K_\lambda$, it acquires a topology from $K_\lambda$ and one from $Q_\ell$, but the two topologies are the same.

The fields $K_\lambda$ with $K$ a number field and $\lambda$ lying above $\ell$ are the only possible finite extensions of $Q_\ell$. If $L$ is one such field then the ring $O_L = O_{K,\lambda}$ is a lattice such that there is a $\mathbb{Z}_\ell$-basis of it which is also a $Q_\ell$-basis for $L$.

Now, let $G$ be the absolute Galois group of $\mathbb{Q}$. Any automorphism $\sigma \in G$ fixes $\mathbb{Q}$ pointwise and, for each Galois number field $F$, restricts to $\sigma_F|_F \in \text{Gal}(F/\mathbb{Q})$. The restriction from $G$ to $\text{Gal}(F/\mathbb{Q})$ is surjective. Moreover if $F \subseteq F'$ then $\sigma_F = \sigma_{F'}|_F$. Conversely, every system of automorphisms $\{\sigma_F\}$ over all Galois number fields $F$, which satisfies the same condition, defines an element of $G$. Hence we can write

$$G = \varprojlim_F \text{Gal}(F/\mathbb{Q}).$$

We can put a topology on $G$, namely the Krull topology; a basis for it is given by

$$\{U_\sigma(F) = \{\sigma \tau : \tau|_F = 1\} : \sigma \in G, F \text{ a Galois number field}\}.$$

As usual we write $U(F)$ instead of $U_1(F)$. Being the inverse limit of finite groups, the topological group $G$ is compact.

Even if the group $G$ is not finite, we can generalize some of the definitions given in the previous section. First we need to recall a definition.

**Definition 2.7.** An algebraic integer is an element of $\bar{\mathbb{Q}}$ that satisfies some monic polynomial with coefficients in $\mathbb{Z}$. The set of algebraic integers is denoted $\bar{\mathbb{Z}}$.

Let $p \in \mathbb{Z}$ be any rational prime and $p \subseteq \bar{\mathbb{Z}}$ a maximal ideal lying above $p$. The decomposition group of $p$ is

$$D_p = \{\sigma \in G : p^\sigma = p\}.$$

In particular each $\sigma \in D_p$ acts on $\frac{\bar{\mathbb{Z}}}{p}$ as $(x + p)^\sigma = x^\sigma + p$. Since $\frac{\bar{\mathbb{Z}}}{p} \simeq \bar{\mathbb{F}}_p$, the action of $D_p$ can be viewed as an action on $\bar{\mathbb{F}}_p$. Let $G_{\bar{\mathbb{F}}_p} = \text{Aut}(\bar{\mathbb{F}}_p)$ be the absolute Galois group of $\bar{\mathbb{F}}_p$. The reduction map $D_p \to G_{\bar{\mathbb{F}}_p}$ is surjective and any preimage $\text{Frob}_p \in D_p$ of the Frobenius automorphism is an absolute Frobenius element over $p$. Hence the Frobenius is defined up to the inertia group of $p$, that is

$$I_p = \{\sigma \in D_p : x^\sigma \equiv x \pmod{p} \ \forall x \in \bar{\mathbb{Z}}\}.$$
If $F$ is a Galois number field, then the restriction $G \to \text{Gal}(F/\mathbb{Q})$ maps an absolute Frobenius element to a corresponding Frobenius element for $F$. As before, two Frobenius elements relative to maximal ideals lying above the same prime $p$ are conjugate:

$$\text{Frob}_p^\sigma = \sigma \text{Frob}_p \sigma^{-1}.$$ 

### 2.2 Galois representations

We shall give some details on Galois representations, in particular over $\mathbb{C}$ and over a $\ell$-adic field. Recall that they are continuous homomorphisms from the absolute Galois group $G$ into complex or $\ell$-adic matrix groups.

As usual, an equivalent way to define a representation is as a $G$-module. In our case, a $d$-dimensional Galois representation is a $d$-dimensional topological vector space $V$ over $L$, where $L$ is either $\mathbb{C}$ or a finite extension of $\mathbb{Q}_\ell$, that is also a $G$-module such that the action

$$V \times G \to V$$

$$(v, \sigma) \mapsto v^\sigma$$

is continuous. If $V'$ is another such representation and there is a continuous $G$-module isomorphism of $L$-vector spaces $V \to V'$ then $V$ and $V'$ are equivalent.

We will now show that any Galois representation $\rho : G \to \text{GL}_d(\mathbb{C})$ has finite image.

**Remark 2.8.** Every $\rho : G \to \text{GL}_d(\mathbb{C})$ factors through $\text{Gal}(F/\mathbb{Q}) \to \text{GL}_d(\mathbb{C})$, where $F$ is a Galois number field.

To prove this, let $V$ be a neighbourhood of the identity matrix $I$ in $\text{GL}_d(\mathbb{C})$, which does not contain any nontrivial subgroup and let $U = \rho^{-1}(V)$. Then $U$ is a neighbourhood of 1 in $G$, thus it contains an open set $U(F)$, where $F$ is a Galois number field. Hence $\rho$ factors through

$$\begin{array}{ccc}
    G & \xrightarrow{\rho} & \text{GL}_d(\mathbb{C}) \\
    & \searrow & \\
    & \nearrow \rho & \\
    G & \xrightarrow{\bar{\rho}} & \text{GL}_d(\mathbb{C})
\end{array}$$

and since $G/\overline{U(F)} \cong \text{Gal}(F/\mathbb{Q})$, the representation $\rho$ induces $\bar{\rho}$ on $\text{Gal}(F/\mathbb{Q})$, which is finite. Hence $\text{Im}(\rho) = \text{Im}(\bar{\rho})$ is finite.

Clearly we can consider other Galois representations, where the field $\mathbb{C}$ is replaced, for instance, by a $\ell$-adic field.
2.3. DELIGNE-SERRE’S THEOREM

**Definition 2.9.** Let $d$ be a positive integer; a $d$-dimensional $\ell$-adic Galois representation is a continuous homomorphism

$$\rho : G \to \text{GL}_d(L)$$

where $L$ is a finite extension field of $\mathbb{Q}_{\ell}$.

If $\rho'$ is another such representation and there is a matrix $m \in \text{GL}_d(L)$ such that for all $\sigma \in G$ it holds

$$\rho'(\sigma) = m^{-1}\rho(\sigma)m$$

then $\rho$ and $\rho'$ are equivalent, and we write $\rho \sim \rho'$.

We now want to evaluate $\rho(\sigma)$ for $\sigma \in G$, and especially for $\sigma = \text{Frob}_p$. This is not - a priori - well defined, since $\text{Frob}_p$ is only defined up to the absolute inertia group $I_p$, and so we can compute $\rho(\text{Frob}_p)$ only if the inertia group satisfies $I_p \subseteq \ker(\rho)$. This condition only depends on the underlying prime $p \in \mathbb{Z}$, since if two maximal ideals $p$ and $p'$ lie above the same prime $p$ then their inertia groups are conjugate and so $I_p \subseteq \ker(\rho)$ if and only if $I_{p'}$ does. Hence we can define a special kind of representations, namely unramified ones, giving conditions only on the rational primes.

**Definition 2.10.** Let $\rho$ be a Galois representation and let $p$ be a prime. Then $\rho$ is unramified at $p$ if $I_p \subseteq \ker(\rho)$ for any $p \subseteq \overline{\mathbb{Z}}$ lying above $p$.

Let $\rho : G \to \text{GL}_d(K)$ be a Galois representation, where $K$ is as at the beginning of this chapter, and $p$ a prime such that $\rho$ is unramified at $p$. Then the image of the Frobenius $\text{Frob}_p$, where $p$ lies over $p$, under the map $\rho$ is a well defined element $F_{\rho,p} \in \text{GL}_d(K)$. Let $P_{\rho,p}$ be its characteristic polynomial, i.e.:

$$P_{\rho,p}(T) = \det(1 - F_{\rho,p}T) = 1 - \text{tr}(F_{\rho,p})T + \cdots + (-1)^d \det(F_{\rho,p})T^d.$$

If we chose another prime $p'$ lying above $p$ then the matrix $F_{\rho,p'}$ would be similar to $F_{\rho,p}$. We will be mainly interested in the computation of the polynomial $P_{\rho,p}$, and the trace and determinant of $F_{\rho,p}$, which hence do not depend on the choice of $p$. From this moment on, we will denote by $F_{\rho,p}$ a representative for the class of the matrices which are image of $\text{Frob}_p$ for some $p$ over $p$, and by $P_{\rho,p}$ its characteristic polynomial.

### 2.3 Deligne-Serre’s Theorem

In this section, we will state the main theorem of this work, proved by Deligne and Serre, that guarantees the existence of a complex Galois representation attached to each weight-1 modular form. Let $G$ denote, as before, the absolute Galois group of $\mathbb{Q}$. 
**Theorem 2.11** (Deligne-Serre). Let $N$ be a positive integer, $\varepsilon$ be a Dirichlet character modulo $N$ such that $\varepsilon(-1) = -1$ and $f$ a nonzero modular form of type $(1, \varepsilon)$ with respect to $\Gamma_0(N)$, that is an eigenform for every $T_p$ such that $p \nmid N$, with eigenvalue $a_p$. Then there exists a Galois representation 

$$\rho : G \to \text{GL}_2(\mathbb{C})$$

that is unramified at all primes $p$ such that $p \nmid N$ and satisfies

$$\text{tr}(F_{\rho, p}) = a_p, \quad \det(F_{\rho, p}) = \varepsilon(p)$$

for all $p \nmid N$. This representation is irreducible if and only if $f$ is a cusp form.

We know from the previous section that one such modular form can be either an Eisenstein series or a cusp form. Hence to approach the demonstration of Deligne-Serre’s Theorem we can separately consider the two cases in which $f$ is an Eisenstein series or $f$ is a cusp form.

If $f$ is an Eisenstein series, then by Theorem 1.33 we may assume that $f = E_{1}^{(\psi, \varphi)}$, where $\psi \varphi = \varepsilon$ and so

$$a_p f = T_p f = (\psi(p) + \phi(p)) f,$$

hence the reducible representation $\rho_\psi \oplus \rho_\varphi$ is attached to $f$ in the sense of the Theorem. Thus, from this moment on, we will assume that $f$ is a cusp form. For cusp forms the following theorem holds (see [4], §2). The second result will be largely used in the proof of Deligne-Serre’s Theorem.

**Theorem 2.12.** Let $f = \sum a_n q^n$ (where $q = e^{2\pi iz}$) be a cusp form on $\Gamma_0(N)$ of type $(k, \varepsilon)$ and let $\sigma$ be an automorphism of the field $\mathbb{C}$. If

$$\sigma(f) = \sum_a \sigma(a_n) q^n,$$

then:

- $\sigma(f)$ is a cusp form on $\Gamma_0(N)$ of type $(k, \sigma \varepsilon)$;
- the eigenvalues of Hecke operators $T_p$ lie in the ring of integers of a number field.

**2.3.1 A result by Rankin**

Before we state the main theorem of this section, we will shortly recall two important functions which are typically expressed as series. Let $\mathcal{P}$ be the set of prime numbers.
2.3. DELIGNE-SERRE’S THEOREM

**Definition 2.13.** The Riemann zeta function of the complex variable $s$ is

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \Re(s) > 1.$$  

The sum in Riemann zeta function converges absolutely. Furthermore, this function can also be expressed as an Eulerian product as follows:

$$\zeta(s) = \prod_{p \in \mathcal{P}} (1 - p^{-s})^{-1}, \Re(s) > 1.$$  

**Definition 2.14.** A Dirichlet series is given by

$$\Phi(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s},$$

where $(a_n)$ is a sequence of complex numbers.

Clearly, the Riemann zeta function is a particular case of Dirichlet series, with $a_n = 1$ for all $n$. We can find another example back in Theorem 1.33 where we defined the Dirichlet series associated to a Dirichlet character $\phi$, where $a_n = \phi(n)$. If, as in these two cases, the sequence $(a_n)$ is totally multiplicative (i.e. $a_{mn} = a_n a_m$ for all $n, m$), then we can express the Dirichlet function as an Eulerian product:

$$\Phi(s) = \prod_{p \in \mathcal{P}} (1 - a_p p^{-s})^{-1}.$$  

We are now ready to prove the main theorem.

**Theorem 2.15.** Let $f$ be a nonzero cusp form of type $(k, \varepsilon)$ with respect to $\Gamma_0(N)$. If $f$ is an eigenfunction for all $T_p$ for $p \nmid N$, with eigenvalues $a_p$, then

$$\sum_{p \nmid N} |a_p|^2 p^{-s}$$

converges for $s > k$ in $\mathbb{R}$ and it is bounded by

$$\sum_{p \nmid N} |a_p|^2 p^{-s} \leq \log \left( \frac{1}{s-k} \right) + O(1) \text{ for } s \to k.$$  

**Proof.** We may assume that $f = \sum_{n=1}^{\infty} a_n q^n$ (where as usual $q = e^{2\pi i \tau}$) is a newform. For $p \nmid N$, let $\phi_p \in \text{GL}_2(\mathbb{C})$ be an element such that $\text{tr}(\phi_p) = a_p$ and $\det(\phi_p) = \varepsilon(p)p^{k-1}$. Hence the Dirichlet series attached to $f$ is

$$\Phi_f(s) = \sum_{n=1}^{\infty} a_n n^{-s} = \prod_{p \nmid N} (1 - a_p p^{-s})^{-1} \prod_{p \mid N} (\det(1 - \phi_p p^{-s}))^{-1}.$$
Let \( L(s) \) be
\[
L(s) = \prod_{p|N} (\det(1 - \phi_p \otimes \bar{\phi}_p p^{-s}))^{-1} =
\prod_{p|N} [(1 - \lambda_p \bar{\lambda}_p p^{-s})(1 - \lambda_p \bar{\mu}_p p^{-s})(1 - \mu_p \lambda_p p^{-s})(1 - \mu_p \bar{\mu}_p p^{-s})]^{-1},
\]
where \( \lambda_p \) and \( \mu_p \) are the eigenvalues of \( \phi_p \). Then it can be shown that
\[
L(s) = H(s)\zeta(2s - 2k + 2) \left( \sum_{n=1}^{\infty} |a_n|^2 n^{-s} \right),
\]
where
\[
H(s) = \prod_{p|N} (1 - p^{-2s+2k-2})(1 - |a_p|^2 p^{-s}).
\]

Rankin showed in [13], §4 that \( \sum_{n=1}^{\infty} |a_n|^2 n^{-s} \) converges for \( \Re(s) > k \) and its product with \( \zeta(2s - 2k + 2) \) extends to a meromorphic form on \( \mathbb{C} \) with only a simple pole at \( s = k \). Now, if \( f \) is a modular form of type \((k, \varepsilon)\) on \( \Gamma_0(N) \) and \( p \mid N \) then it can be shown that
\[
\begin{align*}
&\bullet \ a_p = 0 \text{ if } p^2 \mid N \text{ and } \varepsilon \text{ can be defined modulo } N/p; \\
&\bullet \ |a_p| = p^{(k-1)/2} \text{ if } \varepsilon \text{ cannot be defined modulo } N/p; \\
&\bullet \ |a_p| = p^{k/2-1} \text{ if } p^2 \nmid N \text{ and } \varepsilon \text{ can be defined modulo } N/p.
\end{align*}
\]
In any case, \( |a_p| < p^{k/2} \) when \( p \mid N \), and so \( H(s) \) is a nonzero holomorphic function for \( \Re(s) > k \). Thus \( L(s) \) is meromorphic on \( \mathbb{C} \), holomorphic for \( \Re(s) \geq k \), with the only exception of a simple pole at \( k \) and, for \( s > k \) in \( \mathbb{R} \), the function \( L(s) \) is nonzero.

Let \( g_m(s) = \sum_{p|N} |\text{tr}(\phi_p^m)|^2 p^{-ms} \) and \( g(s) = \sum_{m=1}^{\infty} g_m(s) \). Then \( g(s) \) is a Dirichlet series and for \( \Re(s) \) sufficiently large it holds \( g(s) = \log(L(s)) \). In particular it converges for \( \Re(s) \geq k \), by the following classical theorem of complex analysis.

**Theorem 2.16 (Landau).** Given a Dirichlet series \( g(s) \) with non-negative coefficients, the real point on the line of convergence\(^2\) is a singularity of \( g(s) \).

Since \( L(s) \) has a simple pole at \( s = k \), we have
\[
g(s) = \log \left( \frac{1}{s-k} \right) + O(1) \text{ for } s \to k.
\]
In particular since \( g_1(s) \leq g(s) \) and \( g_1(s) = \sum_{p|N} |a_p|^2 p^{-s} \) then
\[
\sum_{p|N} |a_p|^2 p^{-s} \leq \log \left( \frac{1}{s-k} \right) + O(1) \text{ for } s \to k,
\]
as we wanted. \( \square \)

\(^2\)Remember that the line of convergence for a Dirichlet series is the line \( \{ \sigma = \sigma_C \} \), where \( \sigma_C = \inf \{ \sigma \in \mathbb{R} : g(s) \text{ converges for every } s \text{ with } \Re(s) > \sigma \} \). In particular such a function converges on the half-plane \( \Re(s) > \sigma_C \).
In order to apply this theorem to weight-1 forms, let us give a definition.

**Definition 2.17.** Let \( X \subseteq \mathcal{P} \), where \( \mathcal{P} \) is as above the set of prime numbers. The upper density of \( X \) is

\[
\sup \text{dens}(X) = \limsup_{s \to 1^+} \frac{\sum_{p \in X} p^{-s}}{\log(1/(s-1))}.
\]

**Proposition 2.18.** Assuming the same hypothesis as in Theorem 2.15, if \( f \) has weight \( k = 1 \), for every \( \eta > 0 \) there exist \( X_\eta \subseteq \mathcal{P} \) and a finite set \( Y_\eta \subseteq \mathbb{C} \) such that

\[
\sup \text{dens} X_\eta \leq \eta, \quad a_p \in Y_\eta \forall p \notin X_\eta.
\]

**Proof.** We know that the \( a_p \) are elements of \( \mathcal{O}_K \) with \( K \) a finite extension of \( \mathbb{Q} \). Let \( c \geq 0 \) be a constant and let \( Y(c) \) be the set of the elements \( a \in \mathcal{O}_K \) such that \( |\sigma(a)|^2 \leq c \) for every embedding \( \sigma \) of \( K \) in \( \mathbb{C} \). We can see that \( Y(c) \) is a finite set. Let \( X(c) \) denote the set of the prime numbers \( p \) such that \( a_p \notin Y(c) \). We need to prove that if \( c \) is sufficiently big then \( \sup \text{dens} X(c) \leq \eta \). Now, since also the \( \sigma(a_p) \) are eigenvalues for the \( T_p \), using Theorem 2.15 we have:

\[
\sum_\sigma \sum_p |\sigma(a_p)|^2 p^{-s} \leq [K : \mathbb{Q}] \log \left( \frac{1}{s-1} \right) + O(1) \quad \text{for} \quad s \to 1;
\]

now \( \sum_\sigma |\sigma(a_p)|^2 \geq c \) for \( p \in X(c) \), hence

\[
c \sum_{p \in X(c)} p^{-s} \leq [K : \mathbb{Q}] \log \left( \frac{1}{s-1} \right) + O(1) \quad \text{for} \quad s \to 1,
\]

so \( \sup \text{dens} X(c) \leq \frac{[K : \mathbb{Q}]}{c} \) and it suffices to take \( c \geq \frac{[K : \mathbb{Q}]}{\eta} \). \( \Box \)

We conclude this section recalling an important result, the Chebotarev Density Theorem; for the proof see, for example, [20].

**Theorem 2.19** (Chebotarev Density Theorem). Let \( K \subseteq L \) a Galois extension of number fields and let \( G \) be its Galois group. Let \( C \subseteq G \) be a conjugacy class. Then the set of the unramified primes \( p \) of \( \mathcal{O}_K \) such that the Frobenius element \( \text{Frob}_p \in C \) has density \( \frac{|C|}{|G|} \).

The density in this context is the natural density (see again [20]), that is

\[
d(S) = \lim_{x \to +\infty} \frac{|\{p : |\mathcal{O}_K/p| \leq x, p \in S\}|}{|\{p : |\mathcal{O}_K/p| \leq x, p \in \mathcal{P}_K\}|},
\]

where \( \mathcal{P}_K \) is the set of prime ideals in \( \mathcal{O}_K \).
CHAPTER 2. DELIGNE-SERRE’S THEOREM

Remark 2.20. We could use the natural density instead of the upper density of Definition 2.17 in the statement of Proposition 2.18; it would be still true. (See [4], § 5).

One of the applications of Chebotarev Density Theorem is the following result, which states that a representation $\rho$ of the absolute Galois group $G$ is completely determined by the characteristic polynomials of the Frobenius elements $P_{p,p} = \det(1 - F_{\rho,p}T)$.

Proposition 2.21. Let $X$ be a set of prime numbers of density 1 and let $\rho$ and $\rho'$ be two semisimple representations: $G \to \text{GL}_d(\mathbb{C})$. If for all $p \in X$, $\rho$ and $\rho'$ are unramified at $p$ and $P_{\rho,p} = P_{\rho',p}$, then $\rho$ and $\rho'$ are isomorphic.

2.3.2 $\ell$-adic representations and reduction modulo $\ell$

Let $K$ be a number field such that its integer ring $\mathcal{O}_K$ contains the coefficients $a_p$ and all the $\varepsilon(p)$. We may also assume that $K$ is Galois over $\mathbb{Q}$. Let $L$ be the set of rational prime numbers $\ell$ which split completely in $K$ (that is, the ramification index and the residue degree are 1). For $\ell \in L$ let $\lambda_\ell$ be a maximal ideal of $\mathcal{O}_K$ lying over $\ell$ so that $\mathbb{F}_\ell$ is the corresponding residue field.

Now let us suppose that $K$ be a finite extension of $\mathbb{Q}$, $\lambda$ as before, $\mathcal{O}_\lambda$ the valuation ring which corresponds to $\lambda$, $k_\lambda$ the residue field. Let $f$ be a modular form of type $(k, \varepsilon)$ with respect to $\Gamma_0(N)$.

Definition 2.22. The modular form $f$ is $\lambda$-integral if its Fourier coefficients belong to $\mathcal{O}_K$; we say $f \equiv 0 \pmod{\lambda}$ if its Fourier coefficients belong to $\lambda$. If $f$ is $\lambda$-integral, we say that it is eigenfunction of $T_p$ modulo $\lambda$, with eigenvalues $a_p \in k_\lambda$, if

$$T_p(f) - a_p f \equiv 0 \pmod{\lambda}.$$ 

We will show that there exists a semisimple Galois representation

$$\rho_\ell : G \to \text{GL}_2(\mathbb{F}_\ell)$$

which is unramified outside $N\ell$ (i.e. at all the primes that do not divide $N\ell$) and such that

$$\det(1 - F_{\rho_\ell,p}T) \equiv 1 - a_p T + \varepsilon(p)T^2 \pmod{\lambda_\ell} \text{ if } p \nmid N\ell.$$ 

In order to show this fact, we will use the following theorem, due to Deligne.

Theorem 2.23. Let $f$ be a nonzero modular form of type $(k, \varepsilon)$ on $\Gamma_0(N)$, with $k \geq 2$; let us suppose that $f$ is an eigenfunction for $T_p$, with $p \nmid N$ and eigenvalues $a_p$. Let $K$ be a finite extension of $\mathbb{Q}$ which contains all the $a_p$. 

and $\varepsilon(p)$. Let $\lambda$ and $\ell$ be as above and $K_\lambda$ the completion of $K$ with respect to $\lambda$. Then there exist a semisimple Galois representation

$$\rho_\lambda : G \to \text{GL}_2(K_\lambda)$$

which is unramified outside $N\ell$ and such that

$$\text{tr}(F_{\rho_\lambda,p}) = a_p, \quad \det(F_{\rho_\lambda,p}) = \varepsilon(p)p^{k-1}.$$ 

This theorem will allow us to prove the following result, which applies to a modular form of any weight and attaches to it a representation over a certain finite field. The proof of this theorem, i.e. the construction of the representation $\rho_\lambda$, involves geometric arguments which are not dealt with in this work, namely the $\ell$-adic cohomology of the modular curve of level $N$. For the proof, see [3] and also [10] for a more elaborate study of $\ell$-adic cohomology.

**Theorem 2.24.** Let $f$ be a modular form of type $(k,\varepsilon)$ with respect to $\Gamma_0(N)$, $k \geq 1$. With the above notations, let $f$ be $\lambda$-integral, nonzero modulo $\lambda$, and an eigenfunction for $T_p$ modulo $\lambda$, for $p \nmid N\ell$, with eigenvalues $a_p \in k_\lambda$. Let $k_f$ be the subfield of $k_\lambda$ generated by all the $a_p$ and the reductions modulo $\lambda$ of all $\varepsilon(p)$.

Then there exists a semisimple representation

$$\rho : G \to \text{GL}_2(k_f)$$

which is unramified outside $N\ell$ and such that for $p \nmid N\ell$,

$$\text{tr}(F_{\rho,p}) = a_p, \quad \det(F_{\rho,p}) \equiv \varepsilon(p)p^{k-1} \pmod{\lambda}.$$ 

In particular, when the weight is $k = 1$, we have the previous statement: $\det(1 - F_{\rho,p}T) = 1 - a_pT + \varepsilon(p)T^2$.

**Proof.** First of all, we notice that if $(K',\lambda', f', k', \varepsilon', \{a'_p\})$ satisfies the same hypothesis, and

- $K' \supseteq K$;
- the absolute value defined by $\lambda'$ extends the one induced by $\lambda$;
- $a_p \equiv a'_p \pmod{\lambda'}$;
- $\varepsilon(p)p^{k-1} \equiv \varepsilon'(p)p^{k'-1} \pmod{\lambda'}$,

then the statements for $f$ and for $f'$ are equivalent. To satisfy the last two conditions it suffices to have $\varepsilon' = \varepsilon$, $k' \equiv k \pmod{\ell - 1}$ and $f' \equiv f \pmod{\lambda'}$.

Now let us show that we can suppose that $k \geq 2$. Let $n > 2$ be an even number and let $E_n$ be the Eisenstein series obtained normalizing

$$G_n = \sum_{(c,d) \in \mathbb{Z}^2 \setminus \{(0,0)\}} (cz + d)^{-n}$$

and

$$2.3. \text{DELINE-SERRE'S THEOREM}$$

49
so that the constant term is 1. If \((\ell - 1) \mid n\), then the Fourier coefficients of \(E_n\) are \(\ell\)-integer and \(E_n \equiv 1 \pmod{\ell}\). For a proof of this fact, see \([21]\). Hence \(f E_n \equiv f \pmod{\lambda}\). Furthermore its weight is \(k + n\) and \(k + n \equiv k \pmod{\ell - 1}\). Thus the theorem for \(f E_n\) is equivalent to the theorem for \(f\).

The second assumption we may make is that \(f\) is an eigenform for all the \(T_p\). We want to apply again what is stated at the beginning of the proof, showing that there exists \(f'\) such that \((k', \varepsilon') = (k, \varepsilon)\) and \(f'\) is an eigenform of the \(T_p\). In order to do so, we will use the following lemma.

**Lemma 2.25.** Let \(M\) be a free module of finite type on a discrete valuation ring \(O\); let \(m\) be its maximal ideal, \(k\) the residue field and \(\overline{K}\) the quotient field. Let \(T\) be a set of endomorphisms of \(M\) which commute with each other. Let \(f \in \frac{M}{mM}\) be a common eigenvector of all \(T \in T\), with eigenvalues \(\{a_T\}\) in \(k\).

Then there exists a discrete valuation ring \(O' \supseteq O\), with maximal ideal \(m'\) such that \(m' \cap O = m\) and quotient field \(K'\) which is a finite extension of \(K\), and there exists a nonzero element \(f' \in M \otimes_O O'\) that is an eigenvector for all \(T \in T\), with eigenvalues \(\{a'_T\}\) which satisfy \(a'_T \equiv a_T \pmod{m'}\).

A proof of this lemma may be found in \([4]\), §6. Given this lemma, if \(T\) is the family of the \(T_p\) and \(M\) is the \(O_{\lambda}\)-module of the modular forms with Fourier coefficients in \(O_{\lambda}\) of type \((k, \varepsilon)\) with respect to \(\Gamma_0(N)\), we have that \(f\) is an eigenvector of the reduced action and so there exists a modular form \(f'\) with coefficients in a finite extension \(K'\) of \(K\), which is an eigenfunction for all the \(T_p\).

So, let \(k \geq 2\) and \(f\) be an eigenfunction of all the \(T_p\), for \(p \nmid N\ell\); since \(T_\ell\) and \(T_p\) commute, we can also suppose that \(f\) is an eigenfunction of \(T_\ell\) if \(\ell \nmid N\) (using the same lemma). Let

\[
\rho_\lambda : G \to \text{GL}_2(K_{\lambda})
\]

be the representation attached to \(f\) by Theorem 2.23. We can assume that \(\rho_\lambda(G) \subseteq \text{GL}_2(\mathcal{O}_\lambda)\), where \(\mathcal{O}_\lambda\) is the integer ring of \(K_{\lambda}\), i.e. the completion of \(O_{\lambda}\). Thus, reducing modulo \(\lambda\), we have

\[
\tilde{\rho}_\lambda : G \to \text{GL}_2(k_{\lambda}).
\]

From \(\tilde{\rho}_\lambda\) we can obtain a representation \(\phi\) (called *semisimplification*), which is the direct sum of all the Jordan-Hölder constituents of \(\rho_\lambda\). Such \(\phi\) is unramified outside \(N\ell\), because \(\rho_\lambda\) is, and by Theorem 2.23 it satisfies the two conditions

\[
\text{tr}(F_{\phi, p}) = a_p, \quad \det(F_{\phi, p}) \equiv \varepsilon(p)p^{k-1} \pmod{\lambda} \quad \text{for} \quad p \nmid N\ell.
\]

Since \(\phi(G)\) is finite and \(\phi\) is unramified outside \(N\ell\), by Chebotarev’s Density Theorem, all the elements of \(\phi(G)\) take the form \(\text{Frob}_{p, p}\) for some
prime $p$ with $p \nmid N\ell$. In particular for all $s \in \phi(G)$ the coefficients of\noindent $\det(1 - sT)$ belong to $k_f$, by its definition. Finally we want to apply the\noindent following lemma (see [4], §6).

**Lemma 2.26.** Let $\phi : \Phi \rightarrow \text{GL}_n(k')$ a semisimple representation of a group $\Phi$ over a finite field $k'$; let $k$ be a subfield of $k'$ which contains the coefficients of all the polynomials $\det(1 - \phi(s)T)$ for $s \in \Phi$. Then $\phi$ is realizable over $k$: it is isomorphic to a representation $\rho : \Phi \rightarrow \text{GL}_n(k)$.

Since the condition on the polynomial is satisfied by the elements of $G$, by this lemma there exists $\rho : G \rightarrow \text{GL}_2(k_f)$ as stated in Theorem 2.24

If, as in the beginning of this section, the residue field is $k_\lambda \cong \mathbb{F}_{\ell}$, the representation $\rho$ given by Theorem 2.24 is the one we wanted.

### 2.3.3 A bound on the order of certain subgroups of $\text{GL}_2(\mathbb{F}_{\ell})$

Let $\ell$ be a prime number and let $G$ be a subgroup of $\text{GL}_2(\mathbb{F}_{\ell})$, which can be seen as the group $\text{GL}(V)$ for a 2-dimensional vector space $V$ over $\mathbb{F}_{\ell}$. Given two numbers $\eta$ and $M$, we consider the following property:

$C(\eta,M)$: there exists $H \subseteq G$ such that $|H| \geq (1 - \eta)|G|$ and the set\noindent $\{\det(1 - hT) : h \in H\}$ has at most $M$ elements.

We say that a group $G$ is semisimple if the identical representation $G \rightarrow \text{GL}_2(\mathbb{F}_{\ell})$ is semisimple. It is possible to divide the subgroups of $\text{GL}_2(\mathbb{F}_{\ell})$ into four categories, but first we need to give a definition.

**Definition 2.27.** Let $G$ be a subgroup of $\text{GL}_2(\mathbb{F}_{\ell})$. Then $G$ is a Cartan subgroup if it is one of the following.

- If $V \cong D_1 \oplus D_2$, the split Cartan subgroup defined by $\{D_1, D_2\}$ is formed by the elements $s \in \text{GL}_2(\mathbb{F}_{\ell})$ such that $sD_1 = D_1$ and $sD_2 = D_2$; it is abelian and isomorphic to $\mathbb{Z}/(\ell - 1)\mathbb{Z} \times \mathbb{Z}/(\ell - 1)\mathbb{Z}$.

- If $K$ is a subalgebra of $\text{End}(V)$ which is isomorphic to a field composed of $\ell^2$ elements, then a non-split Cartan subgroup is $K^*$, which is cyclic of order $\ell^2 - 1$.

If $G$ is a semisimple subgroup of $\text{GL}_2(\mathbb{F}_{\ell})$, then one of the following is satisfied:

- $G \supseteq \text{SL}_2(\mathbb{F}_{\ell})$;
- $G$ is contained in a Cartan subgroup $T$;
- $G$ is contained in the normalizer of a Cartan subgroup $T$ and is not contained in $T$;
the image of $G$ in $\mathbb{P} \text{GL}_2(\mathbb{F}_\ell)$ is isomorphic to $A_4$ or $S_4$ or $A_5$ where $S_n$ is the symmetric group on $n$ elements and $A_n$ is the alternating group on $n$ elements.

A proof of this fact may be found in [16], §2. Using this classification, we will be able to prove the following proposition.

**Proposition 2.28.** Let $\eta < \frac{1}{2}$ and $M \geq 0$. Then there exists $A = A(\eta, M)$ such that for every prime number $\ell$ and every semisimple subgroup $G$ of $\text{GL}_2(\mathbb{F}_\ell)$ which satisfies the property $C(\eta, M)$, it holds $|G| \leq A$.

**Proof.** Let us first suppose that $G \supseteq \text{SL}_2(\mathbb{F}_\ell)$. Since $|\text{SL}_2(\mathbb{F}_\ell)| = \ell(\ell^2 - 1)$, we have that $|G| = r\ell(\ell^2 - 1)$, where $r = [G : \text{SL}_2(\mathbb{F}_\ell)]$. The number of matrices in $\text{GL}_2(\mathbb{F}_\ell)$ with given characteristic polynomial is $\ell^2 + \ell$, $\ell^2$ or $\ell^2 - \ell$ if, respectively, the polynomial has 2, 1 or 0 roots in $\mathbb{F}_\ell$.

Hence it holds:

$$r\ell(\ell^2 - 1)(1 - \eta) = |G|(1 - \eta) \leq |H| \leq M(\ell^2 + \ell),$$

so $\ell \leq \frac{M}{r(1 - \eta)} + 1 \leq \frac{M}{1 - \eta} + 1$ and $|G| \leq A_1(\eta, M)$, where

$$A_1(\eta, M) = \frac{M}{1 - \eta} \left( \frac{M}{1 - \eta} + 1 \right) \left( \frac{M}{1 - \eta} + 2 \right).$$

Now, let $G$ be a subset of a Cartan subgroup $T$. At most two of the elements of $T$ (hence of $G$) have a given characteristic polynomial; since $G$ satisfies $C(\eta, M)$ and $1 - \eta > 0$, $(1 - \eta)|G| \leq |H| \leq 2M$ and so

$$|G| \leq A_2(\eta, M) = \frac{2M}{1 - \eta}.$$

In the third case, the group $G' = G \cap T$ has index 2 in $G$, hence $G'$ satisfies $C(2\eta, M)$. Since $2\eta < 1$, we can apply the result of the previous case to $G'$, thus obtaining:

$$|G'| \leq \frac{2M}{1 - 2\eta} \text{ and } |G| \leq A_3(\eta, M) = \frac{4M}{1 - 2\eta}.$$

Finally, let us suppose that the image of $G$ in the projective plane $\mathbb{P} \text{GL}_2(\mathbb{F}_\ell)$ is $A_4$ or $S_4$ or $A_5$. The image of $G$ in $\mathbb{P} \text{GL}_2(\mathbb{F}_\ell)$ has at most order 60, so since $\mathbb{P} \text{SL}_2(\mathbb{F}_\ell)$ has index 2 in $\mathbb{P} \text{GL}_2(\mathbb{F}_\ell)$,

$$|G \cap \text{SL}_2(\mathbb{F}_\ell)| \leq 120.$$
This implies that there are at most 120 matrices with given determinant, hence at most 120 matrices with given characteristic polynomial. If $G$ satisfies $C(\eta, M)$, then as above

$$(1 - \eta)|G| \leq 120M,$$

thus $A_4(\eta, M) = \frac{120M}{1 - \eta}$.

Finally, we set $A(\eta, M) = \max_i\{A_i(\eta, M)\}$.

### 2.3.4 Proof of Deligne-Serre’s Theorem

We are now ready to prove Deligne-Serre’s Theorem; as already noticed, we may assume that the function $f$ is a cusp form of type $(1, \varepsilon)$ on $\Gamma_0(N)$. Let us recall the notation used in Section 2.3.2: $K$ is a Galois number field whose ring of integers contains all the $a_p$ and $\varepsilon(p)$, $L$ is the set of prime numbers $\ell$ that split completely in $\mathcal{O}_K$, $\lambda_\ell$ is a maximal ideal lying over $\ell \in L$ with residue field $F_\ell$, $\rho_\ell : G \rightarrow \text{GL}_2(F_\ell)$ is a representation such that $\det(1 - F_\rho_{\ell,p}T) \equiv 1 - a_pT + \varepsilon(p)T^2 \pmod{\lambda_\ell}$ if $p \nmid N\ell$. Now let $G_\ell$ be the image of $G$ through $\rho_\ell$ in $\text{GL}_2(F_\ell)$. First of all, we will show that such $G_\ell$ has the property $C(\eta, M)$ of Section 2.3.3 (for some $(\eta, M)$), hence the order of $G_\ell$ is bounded by a certain constant $A$.

**Lemma 2.29.** For all $\eta > 0$ there exists a constant $M$ such that every $G_\ell$ with $\ell \in L$ has the property $C(\eta, M)$.

**Corollary 2.30.** There exists a constant $A$ such that $|G_\ell| \leq A$ for every $\ell \in L$.

**Proof of Lemma 2.29** Let $X_\eta$ be as in Theorem 2.18, a subset of $\mathcal{P}$ such that $\sup \text{dens} X_\eta \leq \eta$ and the set of the $a_p$ with $p \notin X_\eta$ is finite. Let $\mathfrak{M}$ be the set of the polynomials $1 - a_pT - \varepsilon(p)T^2$ for $p \notin X_\eta$; this set is finite, and let $M = |\mathfrak{M}|$ be its cardinality. We now claim that, with this choice of $M$, the group $G_\ell$ satisfies the condition $C(\eta, M)$ for every $\ell \in L$. Let $H_\ell$ be the subset of $G_\ell$ given by all the conjugates of the Frobenius elements $F_{\rho_{\ell,p}}$, for $p \notin X_\eta$. Then, by Chebotarev Density Theorem, it holds $|H_\ell| \geq (1 - \eta)|G_\ell|$. Furthermore, for every $h \in H_\ell$, the polynomial $\det(1 - hT)$ is the reduction modulo $\lambda_\ell$ of some element of $\mathfrak{M}$, thus it belongs to a set of at most $M$ elements. Hence $G_\ell$ satisfies the condition $C(\eta, M)$.

Let $A$ be as in Corollary 2.30. Up to taking a finite extension of the field $K$ we may suppose that it contains all the $n$-th roots of unity for $n \leq A$. Let $Y$ be the (finite) set of the polynomials $(1 - \alpha T)(1 - \beta T)$ where $\alpha$ and $\beta$ are $n$-th roots of unity with $n \leq A$. Clearly if $p \nmid N$ then for every $\ell \neq p$ the polynomial $1 - a_pT + \varepsilon(p)T^2$ is equal to some $R(T) \in Y$ modulo $\lambda_\ell$;
in particular, since $Y$ is finite, there is a polynomial $R(T)$ that satisfies the congruence for infinitely-many $\ell$, hence

$$1 - a_p T + \varepsilon(p) T^2 = R(T) \in Y.$$ 

Now let

$$L' = \{ \ell \in L : \ell > A \text{ and it holds } R, S \in Y, R \neq S \Rightarrow R \equiv S \pmod{\lambda_\ell} \}.$$ 

Since $L \setminus L'$ is contained in the set

$$\{ \ell : \ell < A \} \cup \{ \ell : \exists R, S \in Y, R \neq S \text{ and } R \equiv S \pmod{\lambda_\ell} \},$$

it is finite, thus $L'$ is infinite. Let $\ell \in L'$; since $|G_\ell| \leq A < \ell$ and $\ell$ is prime, then the numbers $|G_\ell|$ and $\ell$ are relatively prime; therefore the identical representation $G_\ell \to \text{GL}_2(\mathbb{F}_\ell)$ can be lifted to some representation $G_\ell \to \text{GL}_2(\mathcal{O}_{\lambda_\ell})$, where $\mathcal{O}_{\lambda_\ell}$ is the valuation ring of $\lambda_\ell$ in $K$.

More precisely, the representation modulo $\ell$ lifts to some $G_\ell \to \text{GL}_2(\mathbb{W}(\mathbb{F}_\ell))$, where $\mathbb{W}(\mathbb{F}_\ell)$ is the ring of Witt vectors of $\mathbb{F}_\ell$. In this case, $\mathcal{O}_{\lambda_\ell} = \mathbb{W}(\mathbb{F}_\ell) = \mathbb{Z}_\ell$. A proof of this fact may be found in [7], §4.4 and consists of separately lifting every irreducible component of the initial representation.

Hence

$$\rho : G \to G_\ell \to \text{GL}_2(\mathbb{Z}_\ell)$$

is a representation which is unramified outside $N\ell$. Now, if $p \nmid N\ell$, the Frobenius elements $F_{\rho,p}$ have order at most $A$ (because they belong to $G_\ell$), so the eigenvalues of these elements are roots of unity of order at most $A$. Therefore:

- the polynomial $\det(1 - F_{\rho,p} T) \in Y$. We also know that
  $$\det(1 - F_{\rho,p} T) \equiv 1 - a_p T + \varepsilon(p) T^2 \pmod{\lambda_\ell},$$
  and since they both belong to $Y$ they are equal, and this equality holds for every prime number $p \nmid N\ell$.

- Fixing an embedding $\mathbb{Z}_\ell \hookrightarrow \mathbb{C}$, the representation $\rho$ can be seen as a complex representation.

If $\ell'$ is another element of $L'$, we obtain another representation $\rho' : G \to \text{GL}_2(\mathcal{O}_{\lambda_{\ell'}})$, that satisfies the same properties as $\rho$ for every $p \nmid N\ell'$, in particular

$$\det(1 - F_{\rho,p} T) = \det(1 - F_{\rho',p} T)$$

---

3See [18], §2.6 for the definition
for $p \nmid N\ell'$. By Proposition 2.21 these two representations are isomorphic as representations over $GL_2(K)$ and so as complex representations.

In particular, $\rho$ is unramified outside $N$ and

$$\det(1 - F_{\rho,p}) = 1 - a_p T + \varepsilon(p) T^2 \quad \forall p \nmid N.$$  

We have already proved that if $f$ is an Eisenstein series then the Galois representation attached to it is reducible; we will now prove that if $f$ is a cusp form then $\rho$ is irreducible. By contradiction, let us suppose that $\rho$ is the sum of two 1-dimensional representations, which correspond to the characters $\chi_1$ and $\chi_2$ respectively, are unramified outside $N$ because $\rho$ is, and satisfy $\chi_1 \chi_2 = \varepsilon$ and $\chi_1(p) + \chi_2(p) = a_p$ for $p \nmid N$. Now:

$$\sum_p |a_p|^2 p^{-s} = 2 \sum_p p^{-s} + \sum_p \chi_1(p) \overline{\chi_2(p)} p^{-s} + \sum_p \overline{\chi_1(p)} \chi_2(p) p^{-s}.$$  

We know that $\sum_p p^{-s} = \log \frac{1}{s - 1} + O(1)$ for $s \rightarrow 1^+$. Moreover, $\chi_1 \overline{\chi_2} \neq 1$, otherwise $\varepsilon$ would not be odd, and so the two terms $\sum_p \chi_1(p) \overline{\chi_2(p)} p^{-s}$ and $\sum_p \overline{\chi_1(p)} \chi_2(p) p^{-s}$ are $O(1)$. Therefore:

$$\sum_p |a_p|^2 p^{-s} = 2 \log \frac{1}{s - 1} + O(1) \quad \text{for} \quad s \rightarrow 1^+,$$

in contradiction with Theorem 2.15.

**Remark 2.31.** Thanks to Proposition 2.21, the representation attached to a modular form is unique, up to isomorphism.
Chapter 3

Serre’s Conjecture

In this final chapter, as a natural prosecution of the study of Deligne-Serre’s Theorem we will explain Serre’s Conjecture of 1975. This conjecture states a converse of the theorems of Deligne-Serre (for modular forms of weight 1) and of Deligne (for modular forms of higher weight): given an odd, irreducible representation, this is modular, meaning that it is attached to a modular cusp form.

Serre’s Conjecture has been completely proved by Khare and Wintenberger in 2008, but in this thesis we will not tackle the full problem. For more details, see Khare and Wintenberger’s work in [8] and [9].

Before the Conjecture was completely worked out, it had already been proved in some particular cases, for example when the image of the representation is dihedral and when it is included in $GL_2(F_3)$: we will briefly show how to prove the conjecture in these two cases. Finally, we will show how Fermat’s Last Theorem is related to Serre’s Conjecture.

3.1 Artin conductor

Given an irreducible Galois representation, Serre gives a recipe for the level, character and weight of the modular form to which it is attached. In order to understand it, we need to give the construction of the Artin representation and the definition of the Artin conductor.

Let $K$ and $L$ be two $\ell$-adic fields (finite extensions of $\mathbb{Q}_\ell$, where $\ell$ is prime) such that $L/K$ is a Galois extension with Galois group $G(L/K)$. Let us fix a valuation $v_L$ on $L$ such that $v_L(\pi_L) = 1$ if $\pi_L$ is a uniformizing parameter of $L$. Let the function $i_G : G(L/K) \to \mathbb{Z} \cup \{\infty\}$ be defined as follows. Let $x$ be a generator of $\mathcal{O}_L$ as an $\mathcal{O}_K$-algebra. For $\sigma \in G(L/K)$, we set $i_G(\sigma) = v_L(\sigma x - x)$.

**Definition 3.1.** The ramification groups of $G(L/K)$ are given $G_u$, for all
\( u \in \mathbb{R}^+ \), where
\[
\sigma \in G_u \iff i_G(\sigma) \geq u + 1.
\]

A second family of ramification groups is obtained using a different enumeration called the upper numbering, given by \( G^v = G_u \) if and only if \( v = \phi(u) \), where \( \phi \) is the only function: \( \mathbb{R} \to \mathbb{R} \) with the following properties:

- \( \phi(0) = 0 \);
- \( \phi \) is continuous;
- \( \phi \) is piecewise linear;
- \( \phi'(u) = [G_o : G_u]^{-1} \) when \( u \) is not an integer.

This second family of ramification groups is compatible with passage to the quotient, meaning that \( (G^v_H)^v \) is the image of \( G^v \) in \( \frac{G}{H} \).

For further properties of the ramification groups see [1], §6.4.

Now, let \( \chi \) be a character of \( G(L/K) \), that is an integral combination of irreducible characters.

**Definition 3.2.** The Artin conductor of \( \chi \) is the number
\[
f(\chi) = \sum_{i=0}^{\infty} \frac{g_i}{g_0} (\chi(1) - \chi(G_i)),
\]
where \( g_i = |G_i| \) and \( \chi(G_i) = g_i^{-1} \sum_{s \in G_i} \chi(s) \) is the mean value of \( \chi \) on \( G_i \).

If \( \chi \) is irreducible of degree 1, then there is an alternative definition for the Artin conductor which gives the same value of \( f(\chi) \) as this one. To prove this, we need to introduce the Artin character of \( G(L/K) \), which is defined as follows. For \( \sigma \in G(L/K) \), set
\[
a_G(\sigma) = \begin{cases} 
-f_iG(\sigma) & \sigma \neq 1 \\
f \sum_{s \neq 1} i_G(s) & \sigma = 1.
\end{cases}
\]

Here \( f \) is the residue degree of \( L/K \). We state without proof the following proposition and Artin’s Theorem, which express some basic properties of the Artin conductor and character.

**Proposition 3.3.** The following properties hold.

- Let \( g = |G(L/K)| \). Then
\[
f(\chi) = (a_G, \chi) = \frac{1}{g} \sum_{\sigma \in G} \chi(\sigma) a_G(\sigma).
\]
3.1. ARTIN CONDUCTOR

- Let $K \subseteq L' \subseteq L$ be a tower of Galois extensions, let $\chi'$ be a character of $G(L'/K)$ and let $\chi$ be the corresponding character of $G(L/K)$. Then $f(\chi) = f(\chi')$.

- Let $K \subseteq K' \subseteq L$ and let $\psi$ be a character of $G(L/K')$ and $\psi^*$ the corresponding induced character of $G(L/K)$. Then

$$f(\psi^*) = \psi(1)v_K(d_{K'/K}) + f_{K'/K}f(\psi).$$

Here $f_{K'/K}$ is the residue degree of the extension $K'/K$, while $d_{K'/K}$ is the discriminant of $K'/K$. For a precise definition of the discriminant, see again [1], §1.3.

**Theorem 3.4 (Artin).** If $\chi$ is the character of a representation of $G(L/K)$, then $f(\chi)$ is a positive integer.

To conclude this section we present Artin’s representation, that arises from the Artin character $a_G$.

**Theorem 3.5.** Let $L/K$ be as above and let $G(L/K)$ be its Galois group. Then $a_G$ is the character of a complex linear representation of $G(L/K)$ called the Artin representation.

**Proof.** The character $a_G$ takes the same values on conjugate elements and so is a class function; hence it can be written as $\sum m_\chi \chi$, where $\chi$ are the irreducible characters of $G(L/K)$ and $m_\chi \in \mathbb{C}$. Since

$$m_\chi = (a_G, \chi) = f(\chi),$$

by Artin’s Theorem $m_\chi \in \mathbb{Z}^+$, and so $a_G$ is an integral combination of irreducible characters. □

To construct the Artin representation, we proceed as follows. Let $V_\chi$ be an irreducible representation corresponding to the character $\chi$. Then

$$A_G = \sum_\chi f(\chi)V_\chi$$

is the Artin’s representation, and its character is precisely $a_G$.

There are other conductors of a given finite extension. One possible definition for the conductor of a finite extension $L/K$ is the following.

**Definition 3.6.** Let $c$ be the largest integer such that the ramification group $G_c$ is not trivial. Then the conductor of $L/K$ is

$$f(L/K) = \phi(c) + 1,$$

where $\phi$ is the function in Definition [3.1].
Now let $L/K$ be a Galois extension of arbitrary degree and let $\chi : G(L/K) \to \mathbb{C}^*$ be a continuous character. If $L_\chi$ is the subfield of $L$ fixed by $\ker(\chi)$ then it is a cyclic extension of $K$ and the number $f(L_\chi/K)$ is called the conductor of the character $\chi$, and denoted by $f(\chi)$.

This gives the definition of the Artin conductor of a character, i.e. a 1-dimensional representation. In general, given a Galois extension of local fields $L/K$ and given a representation $\rho : G(L/K) \to \text{GL}(V)$, where $V$ is a finite-dimensional vector space over a finite field $F$ of finite characteristic, the conductor exponent $n(\rho)$ is

$$n(\rho) = \int_{-1}^{\infty} \text{codim}_F(V^\rho(G(L/K))dv.$$ 

Here by $G^v(L/K)$ we denote the ramification group of upper index $v$ of $G(L/K)$.

The conductor $N(\rho)$ is $(\pi_K)^{n(\rho)}$, where $\pi_K$ is a uniformizing parameter for $K$.

We now want to give the definition of the Artin conductor for a representation of the absolute Galois group $G(\bar{K}/K)$ of a global field.

**Definition 3.7.** Let $\rho : G(\bar{K}/K) \to \text{GL}(V)$ be a Galois representation, where $V$ is a finite-dimensional group over a finite field $F$ as above. For every prime $p$ of $K$, fix an embedding $K \hookrightarrow \mathbb{Q}_p$, with respect to which we will embed $G(\bar{K}_p/K_p)$ into $G(\bar{K}/K)$. The Artin conductor of $\rho$ is

$$N(\rho) = \prod_{p, \text{char}(F)=1} p^{n(\rho|_{G(K_p/K_p)})}.$$ 

If $K = \mathbb{Q}$, the Artin conductor is a principal ideal, hence it identifies a natural number.

### 3.2 Statement of Serre’s conjecture

With the statement of Deligne-Serre’s Theorem in mind, we will now give the following definition. As in the previous section, $G$ denotes the absolute Galois group $\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$ and $F$ is a finite field of characteristic $p$.

**Definition 3.8.** A representation $\rho : G \to \text{GL}_2(F)$ is odd if the character $\det \rho : G \to F^*$ is odd. An odd representation $\rho$ is modular if there exists a newform (i.e. a normalized eigenform for all the Hecke operators $T_p$), of some weight $k \geq 2$, level $N$ and character $\varepsilon$, with Fourier coefficients in $F$, such that for all primes $\ell$ which are unramified for $\rho$ and do not divide $Np$, the Frobenius element $F_{\rho,\ell}$ has characteristic polynomial

$$1 - a_{\ell}T + \varepsilon(\ell)\ell^{k-1}T^2.$$ 

In this case, $\rho$ and $f$ are said to be associated.
3.2. STATEMENT OF SERRE’S CONJECTURE

We know from Deligne-Serre’s Theorem that given a modular form of weight 1, there is a representation associated to it; Theorem 2.23 for weight greater or equal than 2 shows that an eigenform $f$ gives rise to an associated representation. In [19], Serre conjectures that the converse holds as well. In particular, his conjecture is the following.

**Conjecture 3.9.** Given an odd irreducible representation $\rho : G \to \text{GL}_2(F)$ modulo $p$, there exists a newform modulo $p$ of level $N(\rho)$, weight $k(\rho)$ and - if $\text{char}(F) > 3$ - character $\varepsilon(\rho)$ which is associated to $\rho$.

First of all, we explain Serre’s recipe for $N(\rho)$, $k(\rho)$ and $\varepsilon(\rho)$. The invariant $N(\rho)$ is the Artin conductor of $\rho$ with the possible factors of $p$ removed.

To describe the character $\varepsilon(p)$, we proceed as follows. Let $\det \rho : G \to F^*$ be the determinant character associated to $\rho$.

**Lemma 3.10.** The conductor of character $\det \rho$ divides $N(\rho)p$.

Let $N = N(\rho)$. By the previous lemma, $\det \rho$ can be identified with a pair of Dirichlet characters

$$
\varepsilon : \left( \frac{\mathbb{Z}}{N\mathbb{Z}} \right)^* \to F^*,
$$

$$
\psi : \left( \frac{\mathbb{Z}}{p\mathbb{Z}} \right)^* \to F^*.
$$

We set $\varepsilon(\rho) = \varepsilon$.

Finally, if we write $\psi(x) = x^{k_0-1}$ for $2 \leq k_0 \leq p$, the integer $k_0$ is such that

$$
k(\rho) \equiv k_0 \pmod{p-1}.
$$

To describe more precisely the weight $k(\rho)$, we must consider the action of a certain quotient of the inertia group; for simplicity, we will now suppose that $p$ is odd.

Let $I_p$ the inertia group of $G$ at $p$ (i.e. the inertia group of any $p$ lying over $p$). Let $W_p$ be the wild inertia subgroup, that is the Galois group of $\overline{\mathbb{Q}}/K_1$, where $K_1$ is the maximal tamely ramified subextension of $\mathbb{Q}/K$.

The subgroup $W_p$ is also equal to the ramification group $G_1$ and to the Sylow $p$-subgroup of $I_p$.

**Lemma 3.11.** The semisimplification $\sigma$ of $\rho$ is tame: $\sigma|_{W_p} = 0$.

---

1We recall that a field extension is tame if the ramification indices are relatively prime to the characteristic of the residue field.
62 \hspace{1cm} \textit{CHAPTER 3. SERRE’S CONJECTURE}

See [15], Lemma 21.5.1.

Let $I_t$ be the quotient $\frac{I_p}{W_p}$. By the previous lemma, $I_t$ acts on the semisimplification of $\rho$; now $I_t$ is abelian, because it is isomorphic to $\lim_{\leftarrow} F^*_{p^n}$ (for a proof see again [1], §6.4), so the action of $I_t$ on the semisimplification of $\rho$ is reducible and corresponds to two characters, namely $\chi$ and $\chi': I_t \to \overline{F}_p^*$, which are stable under the action of the Frobenius because the representation $\rho$ extends to the decomposition group $D_p$. Now, since $I_t \cong \lim_{\leftarrow} F^*_{p^n}$, for every $n$ we have maps $I_t \to F^*_{p^n}$, called fundamental characters of level $n$. The unique fundamental character of level 1 is the mod $p$ cyclotomic character.

Let $\psi$ and $\psi'$ be the fundamental characters of level 2 and $\chi_p$ the fundamental character of level 1. Then we have two cases to consider.

- If $\chi^p = \chi'$ and $\chi'^p = \chi$, then we can write
  \[ \chi = \psi^a + \psi'^b, \]
  with $0 \leq a < b \leq p - 1$. Then set
  \[ k(\rho) = 1 + ap + b. \]

- If $\chi^p = \chi$ and $\chi'^p = \chi'$, then we can write
  \[ \rho|_{I_p} = \begin{pmatrix} \chi^p & * \\ 0 & \chi'^p \end{pmatrix}. \]
  If $* = 0$ then $0 \leq a, b \leq p - 2$, and in this case we set $k(\rho) = 1 + pa + b$.
  Otherwise, $0 \leq a \leq p - 1$, $0 \leq b \leq p - 2$ and we set
  \[ - k(\rho) = 1 + p(\min\{a, b\}) + \max\{a, b\} + p - 1 \text{ if } \chi^a - b = \chi_p \text{ and } \rho \otimes \chi_p^{-b} \text{ is finite\footnote{See [15], §21.5.5.} at } p; \]
  \[ - k(\rho) = 1 + p(\min\{a, b\}) + \max\{a, b\} \text{ otherwise. } \]

3.3 \hspace{1cm} \textit{Serre’s epsilon-conjecture}

A weaker statement of Serre’s conjecture known as \textit{Serre’s epsilon-conjecture} is a first step towards its proof.

\textbf{Conjecture 3.12} (Serre’s epsilon-conjecture). If $\rho$ is modular, then it is associated to a modular form modulo $p$ of level $N(\rho)$, weight $k(\rho)$ and - if $p > 3$ - character $\varepsilon(\rho)$.
Here, \(N(\rho), k(\rho)\) and \(\varepsilon(\rho)\) are the ones found in the previous section. In other words, Serre’s epsilon-conjecture states that if we already know that a representation is attached to a modular form, then we can also compute its level, weight and character.

The first known results about the epsilon-conjecture are two theorems by Mazur and Ribet. We will state them without proof, which can be found in Ribet’s work in [14]. In the following, \(G\) will denote as always the absolute Galois group \(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})\). We recall that a representation \(G \to \text{GL}_n(F)\) over a field \(F\) is called absolutely irreducible if it is irreducible over the algebraic closure of \(F\).

**Theorem 3.13** (Mazur). Suppose that \(\rho : G \to \text{GL}_2(F)\) is absolutely irreducible and arises from an eigenform modulo \(p\) of weight 2, level \(N\) and trivial character. If \(\ell \mid| N\) (i.e. \(\ell \mid N\) but \(\ell^2 \nmid N\) and \(\rho\) is finite at \(\ell\) and \(\ell \not\equiv 1 \pmod{p}\), then \(\rho\) arises from a modulo \(p\) eigenform on \(X_0(N/\ell^3)\).

**Theorem 3.14** (Ribet). Suppose that \(\rho : G \to \text{GL}_2(F)\) is absolutely irreducible and arises from an eigenform modulo \(p\) of weight 2, level \(N\) and trivial character. Suppose also that \(\text{char}(F)\) is odd. If \(\ell \mid| N\) and \(\rho\) is finite at \(\ell\), then \(\rho\) arises from a modular form of level \(N/\ell\).

The importance of the theorems of Mazur and Ribet lies in the fact that they are the starting point for the proof of Serre’s epsilon-conjecture. Their work is mainly concerned with modular forms of weight 2 and trivial character; a great number of mathematicians have tried to extends these results to arbitrary weights, levels and characters. Between them F. Diamond almost completely proved Serre’s epsilon conjecture, except for a pair of cases known as exceptional. As before, let \(\rho : G \to \text{GL}_2(F)\) be an irreducible representation arising from an eigenform.

**Definition 3.15.** The representation \(\rho\) is an exceptional case if \(\text{char}(F) = 3\) and \(\rho\) is induced from a character of \(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(\sqrt{-3}))\), or if \(\text{char}(F) = 2\) and \(\rho\) is induced from a character of \(\text{Gal}(\bar{\mathbb{Q}}/\mathbb{Q}(i))\).

**Theorem 3.16** (Diamond). Assume \(F\) is a field of odd characteristic. If \(\rho : G \to \text{GL}_2(F)\) is a representation arising from an eigenform, then \(\rho\) is associated to an eigenform of level \(N(\rho)\), weight \(k(\rho)\) and, if \(\rho\) is not an exceptional case, character \(\varepsilon(\rho)\).

**Proof.** See [5].

### 3.4 Examples

In this section we shall give the general idea of the proof in two simple cases, namely the case where \(\rho\) has dihedral image and the case where \(F = \mathbb{F}_3\),

---

\(^4\)See [6], §2 for the definition of \(X_0(N/\ell)\).
although the conjecture is known in every case. We will follow the paper by H. Darmon (see [2]).

### 3.4.1 Case where \(\rho\) has dihedral image

Let \(\rho : G \to \text{GL}_2(F)\) be an irreducible, odd representation with \(\text{Im}(\rho) \cong D_{2n}\), the dihedral group with \(2n\) elements, and suppose \((n,p) = 1\), where \(p\) is the characteristic of the field \(F\). Then, seeing \(D_{2n}\) as a group of linear transformations of \(\mathbb{C}^2\), we have that \(\rho\) gives rise to a complex representation 

\[
\rho' : G \to D_{2n} \hookrightarrow \text{GL}_2(\mathbb{C}).
\]

Now, if \(\rho\) is odd, then also \(\rho'\) can be assumed to be odd. This representation is associated to a cusp form of weight 1, through a construction that was known already to Hecke. The idea is the following: let \(L\) be the subfield of \(\overline{\mathbb{Q}}\) that is fixed by the kernel of \(\rho\): it is an abelian extension of a quadratic extension \(K\) over \(\mathbb{Q}\), with Galois group a cyclic group of order \(n\), as in the following diagram:

\[
\begin{array}{c}
L \\
\downarrow_{n \text{ (cyclic)}} \\
K \\
\downarrow^2 \\
\mathbb{Q}
\end{array}
\]

Now \(\rho\) can be written as the representation induced by a nontrivial 1-dimensional character \(\chi : \text{Gal}(L/K) \to \mathbb{C}^*\). Hecke proved that the theta-function \(\theta_\chi\) associated to \(\chi\) is a cusp form of weight 1 and level equal to the norm of the discriminant of the field \(L^\tau\), i.e. the subfield of \(L\) fixed by any reflection \(\tau \in \text{Gal}(L/\mathbb{Q})\). Let \(\omega\) be the Teichmüller character at \(p\), i.e. the homomorphism of multiplicative groups \(\omega : \mathbb{F}_p^* \to \mathbb{Z}_p^*\) such that \(\omega(a)\) is the unique \((p-1)\)th root of unity in \(\mathbb{Z}_p\) which is congruent to \(a\) modulo \(p\). By multiplying \(\theta\) by an Eisenstein series of weight 1, level \(p\) and character \(\omega^{-1}\), we obtain a form of weight 2 which is an eigenform for the Hecke operators modulo \(p\), hence by the results of the previous chapter \(\rho\) is modular. Finally, by Theorem 3.16, \(\rho\) is associated to a modular form of weight \(k(\rho)\), level \(N(\rho)\) and if \(\rho\) is not an exceptional case, character \(\varepsilon(\rho)\).

**Remark 3.17.** If the field \(F = \mathbb{F}_2\), the image is still dihedral, so by Hecke’s argument we can prove that \(\rho\) is modular. However, \(\rho\) is an exceptional case and so Serre’s epsilon-conjecture is unproven. According to H. Darmon, it is currently unclear whether there exists a modular form of character \(\varepsilon(\rho)\) associated to \(\rho\).
3.5. FERMAT’S LAST THEOREM

3.4.2 Case where $F = \mathbb{F}_3$

A very similar procedure applies to the case where $F = \mathbb{F}_3$. The full group $GL_2(F)$ can be embedded into $GL_2(\mathbb{C})$, thus obtaining a characteristic 0 representation $\rho' : G \to GL_2(\mathbb{C})$. Langlands and Tunnel (in [11] and [22]), show that $\rho'$ is associated to a modular form of weight 1. Again, by multiplying this modular form by an Eisenstein series, we find a modular form associated to $\rho$. Hence $\rho$ is modular and, by Theorem 3.16, it is associated to an eigenform of weight $k(\rho)$, level $N(\rho)$ and, if $\rho$ is not an exceptional case, character $\varepsilon(\rho)$.

3.5 Fermat’s Last Theorem

We will now briefly explain the relation between Fermat’s Last Theorem and Serre’s Conjecture, giving the general idea for a proof of this theorem.

Let us consider Fermat’s equation

$$a^\ell + b^\ell + c^\ell = 0,$$

where $\ell$ is a prime number, $\ell \geq 5$; a nontrivial solution to this equation would give rise to the Frey curve

$$E : y^2 = x(x - a^\ell)(x + b^\ell).$$

We may assume that $\gcd(a, b, c) = 1$, $a \equiv -1 \pmod{4}$ and $b$ is even. The Frey curve is an elliptic curve and, under these hypotheses, is semistable. We can consider the mod $p$ representation

$$\rho : G \to \text{Aut}(E_p),$$

where $E_p$ is the $p$-torsion of $E$; it holds $\text{Aut}(E_p) \cong GL_2(\mathbb{F}_p)$ and $\rho$ is irreducible. A proof for this fact may be found in [14], §22.1. Using the recipe given in Section 3.2, we can compute $N(\rho) = 2$, $k(\rho) = 2$ and $\varepsilon(\rho) = 1$. Now, since $S_2(\Gamma_0(2)) = \{0\}$ (see [6], §9), the representation $\rho$ cannot be modular. Thus Serre’s Conjecture, if true, implies Fermat’s Last Theorem: there are not any nontrivial solutions of Fermat’s equation. Actually, thanks to Ribet’s work on the epsilon-conjecture we have a stronger result: the representation $\rho$ is modular (hence attached to a form of any level, weight and character) and we can apply Ribet’s Theorem to it, thus proving Fermat’s Last Theorem.
Bibliography


